

Configura Azure Entra Captive Portal su Secure Firewall

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Diagramma](#)

[Portale vincolato tra endpoint, FTD e Azure Entra](#)

[Configurazione](#)

[Fase 1: Configurazione iniziale di FMC e DNS](#)

[Passaggio 1: Abilitare Cisco Dynamic Attributes Connector \(CSDAC\)](#)

[Passaggio 2: Creazione di un oggetto di rete con nome di dominio completo rappresentativo dell'interfaccia in ingresso FTD](#)

[Passaggio 3: Configurare il record A DNS](#)

[Fase 2: Configurazione infrastruttura a chiave pubblica](#)

[Passaggio 1: Importare il certificato CA interno nel CCP](#)

[Passaggio 2: Firmare il certificato del provider di servizi con la CA](#)

[Passaggio 3: Distribuire il certificato SP nell'FTD](#)

[Fase 3: Configurazione di Azure](#)

[Passaggio 1: Creare l'applicazione Entra Enterprise per il toolkit SAML](#)

[Passaggio 2: Configura registrazioni app Entra ID](#)

[Passaggio 3: Configurare le autorizzazioni API di Microsoft Graph per la registrazione dell'app.](#)

[Passaggio 4: Configurare lo spazio dei nomi EH \(Event Hub\)](#)

[Passaggio 5: Scegliere o creare criteri di accesso condiviso nello spazio dei nomi dell'hub eventi](#)

[Passaggio 6: Raccogliere e annotare informazioni sulla firma di accesso condiviso \(SAS\) dallo spazio dei nomi EH](#)

[Passaggio 7: Creare un'istanza dell'hub eventi nello spazio dei nomi dell'hub eventi](#)

[Passaggio 8: Creare un gruppo di consumer dell'istanza dell'hub eventi nello spazio dei nomi dell'hub eventi](#)

[Passaggio 9: Verifica valori raccolti](#)

[Passaggio 10: Configura streaming registro di controllo ID entri nell'hub eventi](#)

[Fase 4: Consolidamento della configurazione di Azure e dell'autenticazione attiva FMC/FTD](#)

[Passaggio 1: Configurare il realm di Azure SAML/Entra ID utilizzando la procedura guidata FMC](#)

[Passaggio 2: Implementare i metadati di SP SAML configurati da FMC nell'applicazione Azure Enterprise](#)

[Passaggio 3: Configurare il realm di Azure SAML/Entra ID utilizzando la procedura guidata di Gestione risorse cluster \(continua\)](#)

[Passaggio 4: Controlla utenti scaricati](#)

[Fase 5: Configurare i criteri in FMC](#)

[Passaggio 1: Configura criterio di decrittografia](#)

[Passaggio 2: Configura regole dei criteri di decrittografia](#)

[Passaggio 3: Crea criterio di identità](#)

[Passaggio 4: Configura regole dei criteri di identità](#)

[Passaggio 5: Configurare i criteri di controllo di accesso](#)

[Passaggio 6: Distribuire le configurazioni sui dispositivi Cisco Secure Firewall](#)

[Verifica](#)

[GUI](#)

[CLI](#)

[Risoluzione dei problemi](#)

[Debug Captive Portal](#)

[Dump identità utente](#)

[Problemi possibili](#)

[Autorità di certificazione sconosciuta del portale vincolato](#)

[Portale vincolato "Server non trovato"](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la configurazione di Microsoft Azure Entra ID per l'utilizzo con il portale captive (autenticazione attiva) su Cisco Secure Firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SAML (Security Assertion Markup Language)
- Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

È necessario che il piano tariffario Standard sia disponibile in Azure per la creazione di hub eventi. Inoltre, i dispositivi devono essere attivati con Smart Licensing abilitato con funzionalità di controllo dell'esportazione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Secure FTD versione 10.0
- Cisco Secure FMC versione 10.0

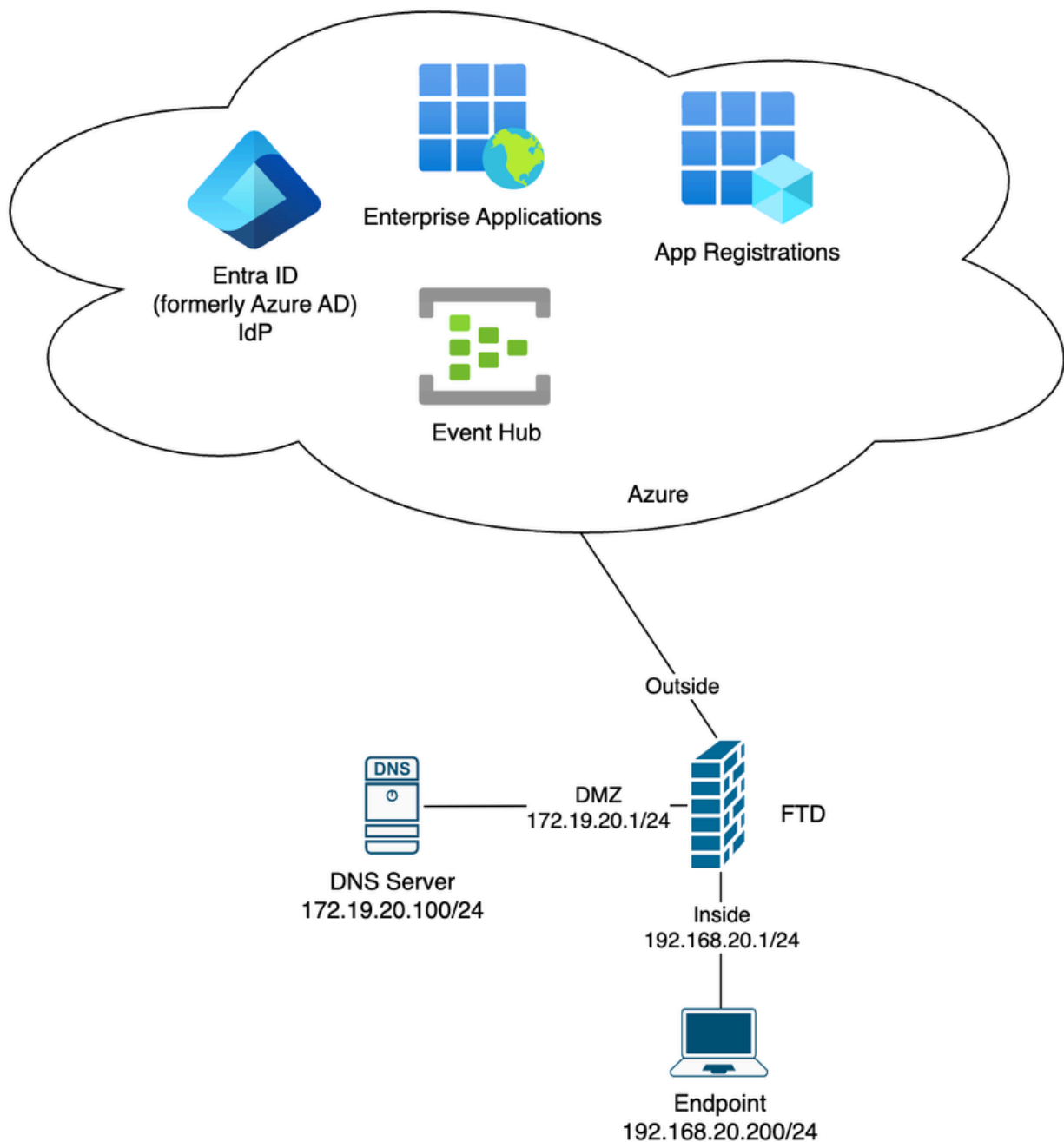
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Poiché le tradizionali architetture di sicurezza basate su IP faticano a tenere il passo con ambienti di lavoro dinamici e ibridi, Cisco Secure Firewall Active Authentication con integrazione SAML offre una soluzione solida e incentrata sull'identità. Utilizzando Microsoft Entra ID (Azure AD) come provider di identità centralizzato, questa configurazione consente agli amministratori di superare le regole di rete statiche e applicare un controllo di accesso granulare basato sull'identità utente verificata anziché sugli indirizzi di rete volatili. Questa integrazione semplifica l'esperienza dell'utente tramite SSO (Single Sign-On) e MFA (Multi-Factor Authentication) obbligatori, garantendo al contempo una postura di sicurezza unificata che mantiene una rigida visibilità e l'applicazione delle policy su una rete senza perimetro.

Diagramma

Portale vincolato tra endpoint, FTD e Azure Entra



Portale vincolato tra EndPoint e Azure Entra

Configurazione

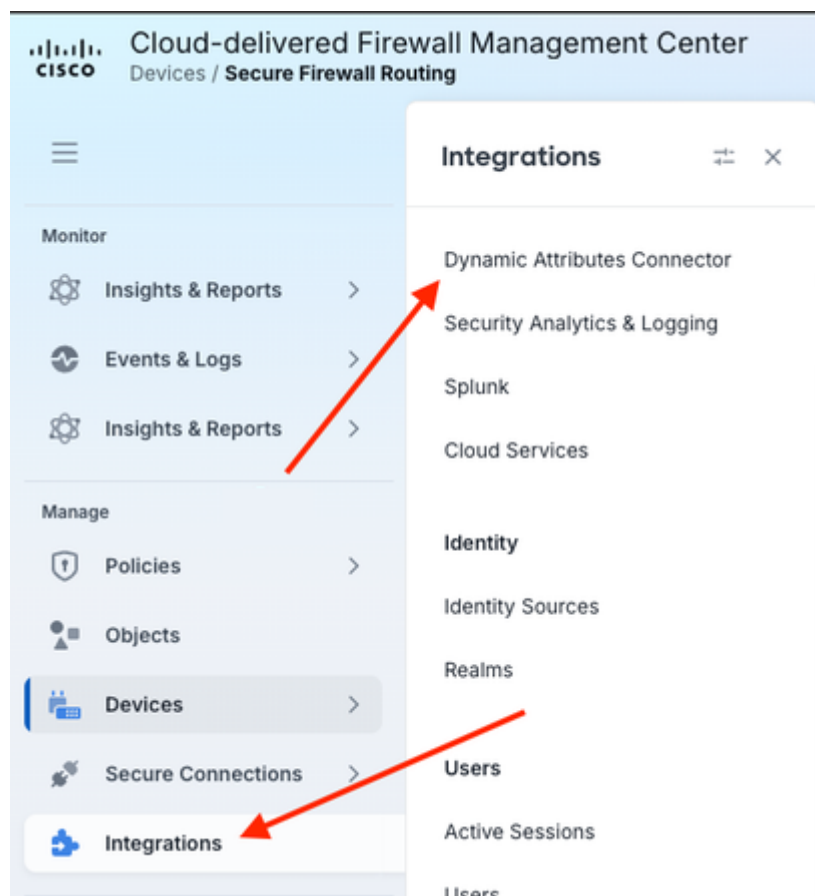
Fase 1: Configurazione iniziale di FMC e DNS



Nota: Questa esercitazione utilizza un centro di gestione dei firewall (cdFMC) distribuito su cloud; le misure restano tuttavia invariate per i CCP locali.

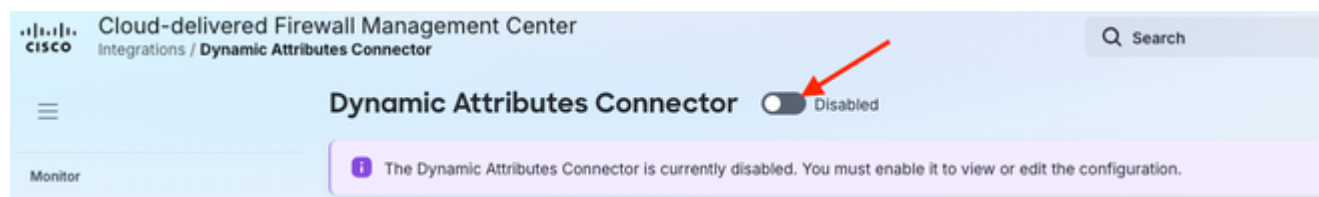
Passaggio 1: Abilitare Cisco Dynamic Attributes Connector (CSDAC)

1) Scegliere Integrations > Dynamic Attributes Connector.



Scegli connettore attributi dinamici integrazioni

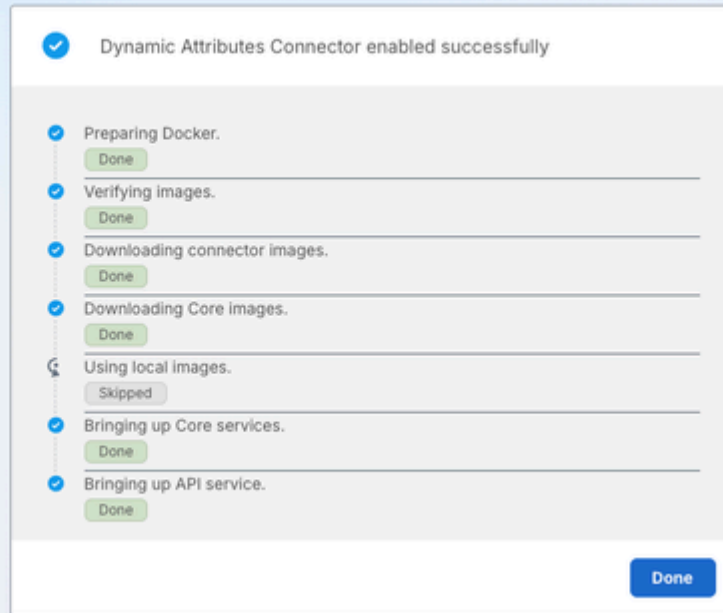
2) Fare clic sul controllo adiacente alla stringa Disabled per abilitare CSDAC.



Abilita Cisco Dynamic Attributes Connector

c) Fare clic su Done (Fine) una volta completata l'attivazione di CSDAC.

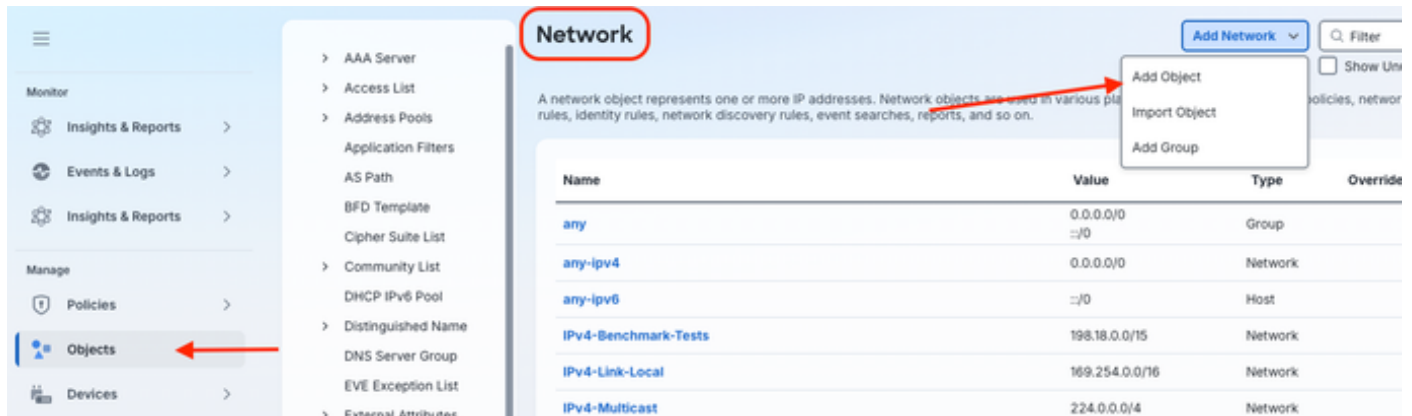
Dynamic Attributes Connector



Abilita stato Cisco Dynamic Attributes Connector

Passaggio 2: Creazione di un oggetto di rete con nome di dominio completo rappresentativo dell'interfaccia in ingresso FTD

1) Scegliere Oggetti > Aggiungi rete > Aggiungi oggetto.



Crea nuovo oggetto di rete con nome di dominio completo

2) Assegnare un nome all'oggetto di rete configurato con il nome di dominio completo (FQDN). Immettere il nome di dominio completo e assegnare l'oggetto di rete come tipo di nome di dominio completo facendo clic sul pulsante di opzione appropriato. Fare clic su Save (Salva).

Edit Network Object ?

Name

Description

Network
☐ Host ☐ Range ☐ Network ☒ FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

☐ Allow Overrides

Cancel Save

Configura variabili oggetto di rete FQDN

Passaggio 3: Configurare il record A DNS

1) Nell'esempio riportato viene utilizzato Windows Server 2025; consultare la documentazione relativa al server di risoluzione dei nomi specifico, se necessario.

DNS			
DC	Name	Type	Data
Forward Lookup Zones	(same as parent folder)	Start of Authority (SOA)	[1], dc., hostmaster.
example.com	(same as parent folder)	Name Server (NS)	dc.
Reverse Lookup Zones	ftd-inside	Host (A)	192.168.20.1
Trust Points			



Nota: Il client che esegue l'autenticazione attiva deve essere in grado di risolvere questo record A DNS.

Fase 2: Configurazione infrastruttura a chiave pubblica

È possibile utilizzare un'Autorità di certificazione (CA) interna come infrastruttura a chiave pubblica (PKI) per la configurazione di autenticazione attiva. Cisco FMC e FTD richiedono il caricamento della chiave pubblica della CA interna e della chiave privata associata come oggetto CA interno per eseguire le necessarie operazioni di intercettazione SSL e di revoca della crittografia. Inoltre, la CA interna deve essere considerata attendibile nel browser client da cui viene eseguita l'autenticazione attiva. Vedere la documentazione del browser client per verificare come il browser consideri attendibile il certificato.

Passaggio 1: Importare il certificato CA interno nel CCP

1) Scegliere Oggetti > PKI > CA interne. Fare clic su Importa CA.



Nota: La CA interna può anche essere creata direttamente sul CCP.

Import Internal Certificate Authority ?

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

Key or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

☒ Encrypted, and the password is:



Nota: All'interno del contenuto di questo documento, viene visualizzato uno spazio bianco che copre i vari valori dei campi nelle immagini ed è intenzionale per la pubblicazione di questo documento. I valori effettivi vengono rispecchiati per l'ambiente in uso durante la configurazione.

Passaggio 2: Firmare il certificato del provider di servizi con la CA

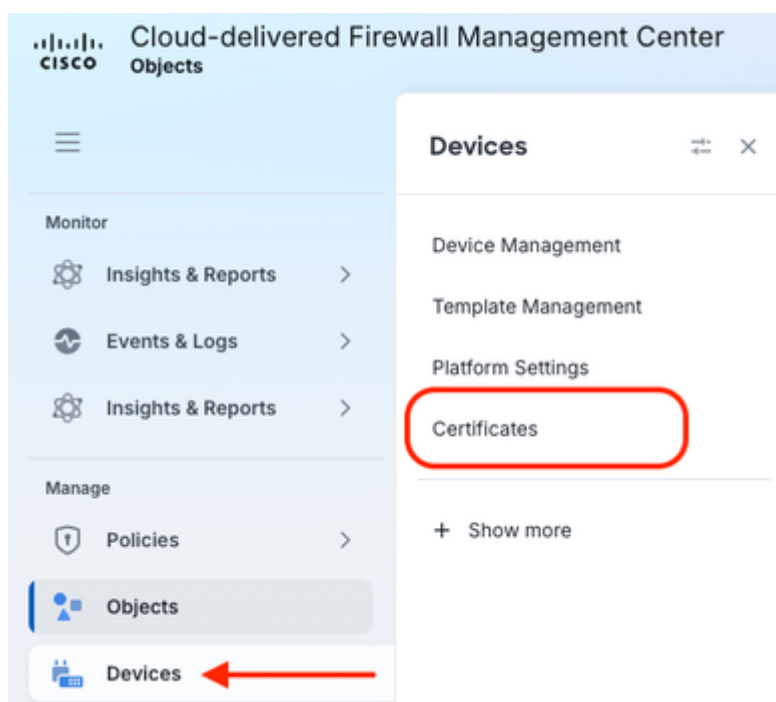
1) Il certificato del provider di servizi (SP) deve essere firmato da un'Autorità di certificazione (CA) attendibile e restituito in formato PKCS#12 (.p12).



Nota: Questa CA può essere firmata internamente. L'unica avvertenza è che la CA interna deve essere considerata attendibile dal dispositivo client.

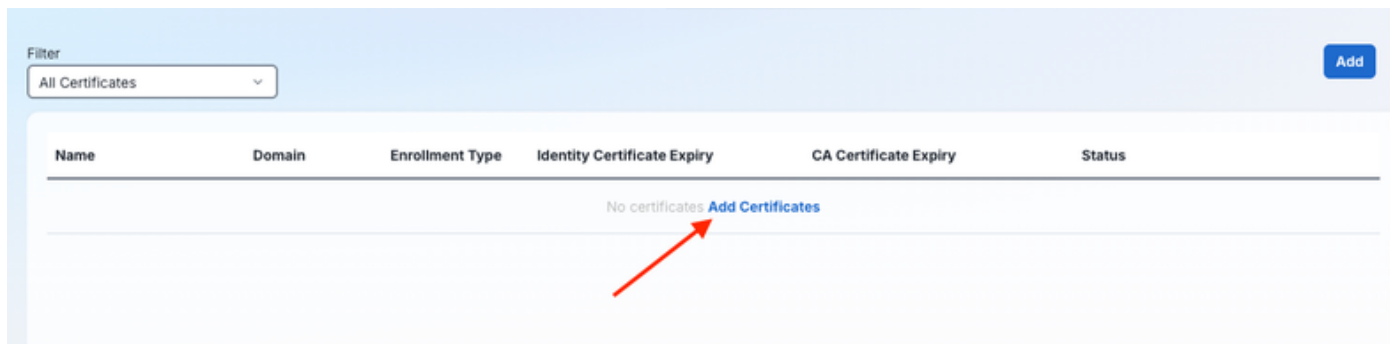
Passaggio 3: Distribuire il certificato SP nell'FTD

1) Scegliere Dispositivi > Certificati.



Passa A Dispositivi E Certificati

2) Fare clic su Add Certificates (Aggiungi certificati).



Aggiungi nuovo certificato dispositivo

3) Selezionare il dispositivo dall'elenco a discesa che esegue l'autenticazione attiva, quindi fare clic sull'icona + per creare una nuova registrazione certificati.

A screenshot of the 'Add New Certificate' form. The title 'Add New Certificate' is at the top left, with a help icon (?) to its right. Below the title is a descriptive text: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' There are two dropdown menus: 'Device*' and 'Certificate Enrollment*'. The 'Device*' dropdown is set to 'FTD', and a red arrow points to it. The 'Certificate Enrollment*' dropdown is empty, and a red arrow points to a '+' button located to its right. At the bottom right of the form are two buttons: 'Cancel' and 'Add'.

Selezionare FTD e Aggiungi nuova registrazione certificato

4) Assegnare un nome alla registrazione certificato e dall'elenco a discesa Tipo di registrazione scegliere file PKCS12.

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

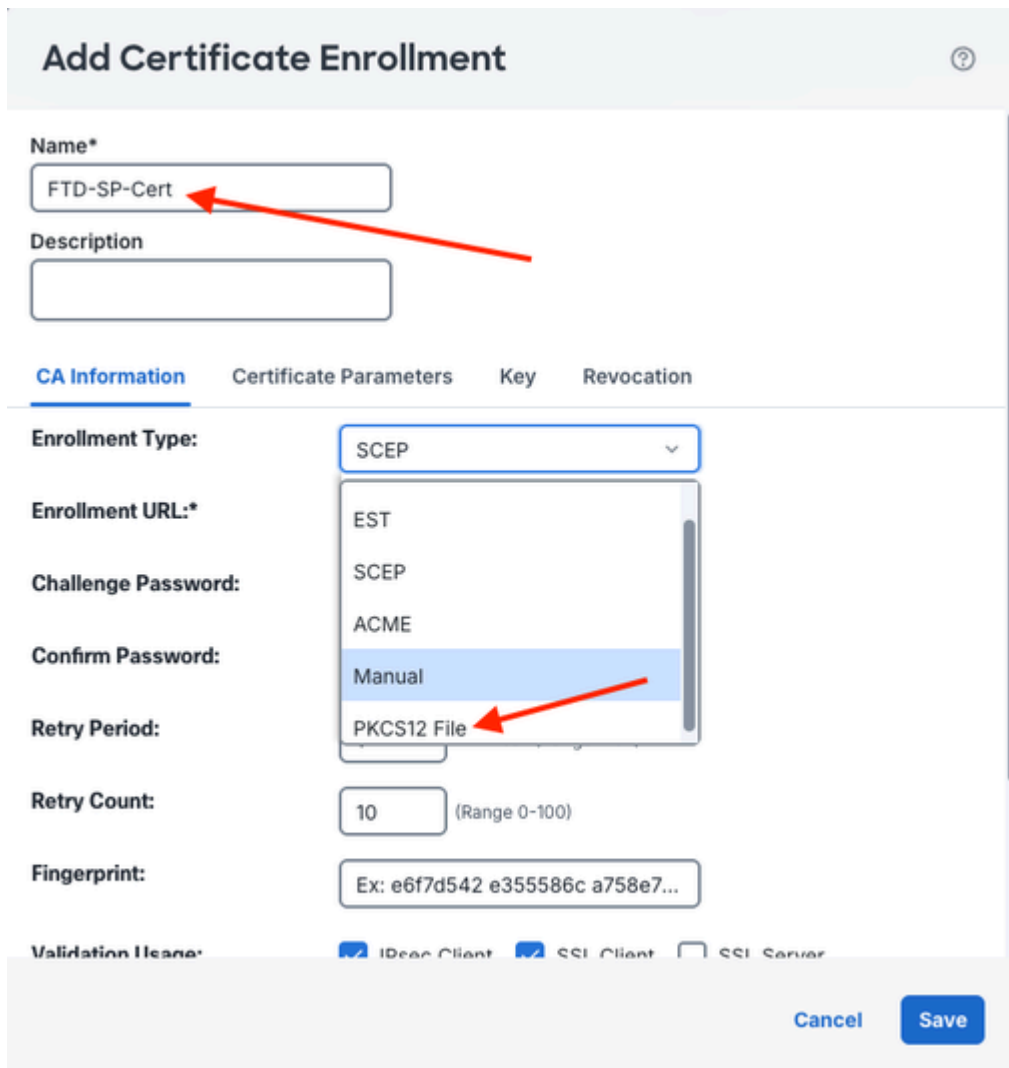
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

Validation Usage: ☒ IDsec Client ☒ SSL Client ☐ SSL Server

Cancel Save



Impostazioni E Tipo Di Registrazione Certificati

5) Importare il file PKCS#12 facendo clic su Sfoglia file PKCS12 e immettere la passphrase richiesta. Fare clic su Save (Salva).

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: SP.p12 [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: ☒ IPsec Client ☒ SSL Client ☐ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☒ Allow Overrides

> Override (0)

Cancel Save

Sforgia e importa file PKCS12

6) Confermare che i dettagli dell'iscrizione siano corretti e fare clic su Aggiungi.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD

Certificate Enrollment*: FTD-SP-Cert +

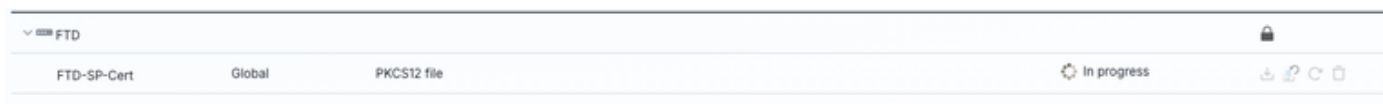
Certificate Enrollment Details:

Name:	FTD-SP-Cert
Enrollment Type:	PKCS12 file
Enrollment URL:	N/A

Cancel Add

Conferma dettagli registrazione certificato

7) L'importazione riflette in corso.



FTD-SP-Cert	Global	PKCS12 file	In progress
-------------	--------	-------------	-------------

Al termine dell'importazione, le informazioni del certificato SP possono essere convalidate facendo clic sull'icona ID del certificato configurato.



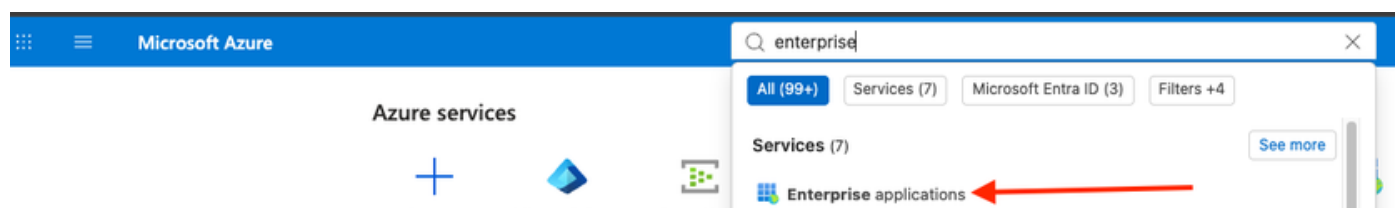
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	 

Stato importazione certificati in corso

Fase 3: Configurazione di Azure

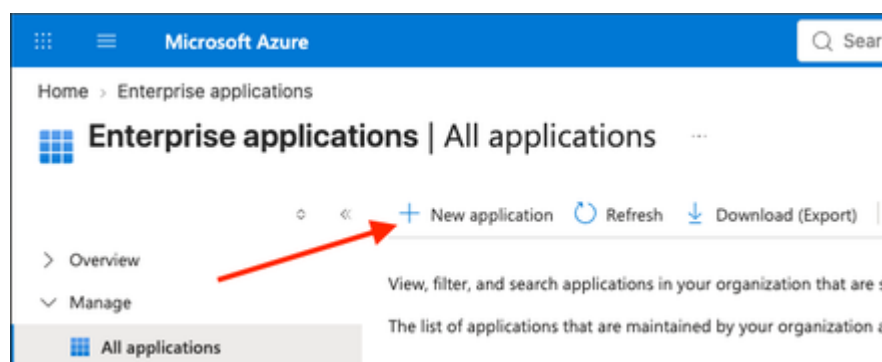
Passaggio 1: Creare l'applicazione Entra Enterprise per il toolkit SAML

1) Cercare e fare clic su Applicazioni aziendali.



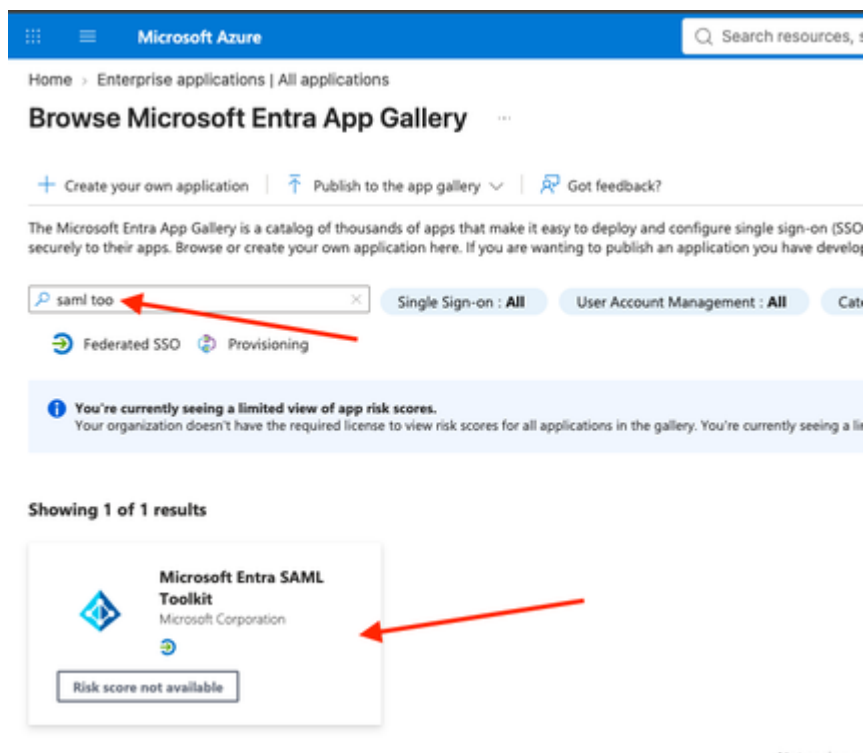
Ricerca E Accesso Alle Applicazioni Aziendali

2) Fare clic su + Nuova applicazione.



Seleziona nuova applicazione nelle applicazioni enterprise

3) Cercare Microsoft Entra SAML Toolkit e fare clic sulla miniatura corrispondente.

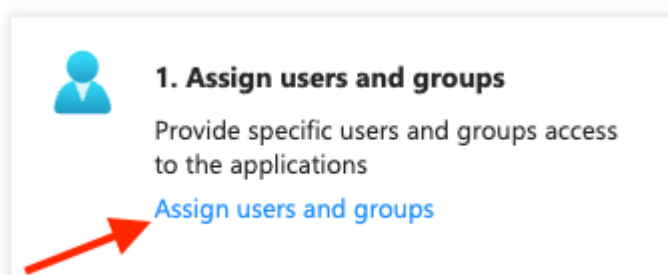


Cerca e seleziona Microsoft Entra SAML Toolkit

4) Assegnare un nome all'applicazione Microsoft Entra SAML Toolkit Enterprise e fare clic su Crea. (Riferimento da Microsoft: [Leggi l'esercitazione dettagliata sull'integrazione di Microsoft Entra SAML Toolkit](#) (esercitazione)).

Assegna nome all'applicazione SAML Toolkit

5) Nella pagina Panoramica, assegnare gli utenti e i gruppi specifici all'applicazione SAML Toolkit Enterprise. In questo esempio, l'account di test (utente-portale vincolato) è un membro del gruppo active-auth-lab.

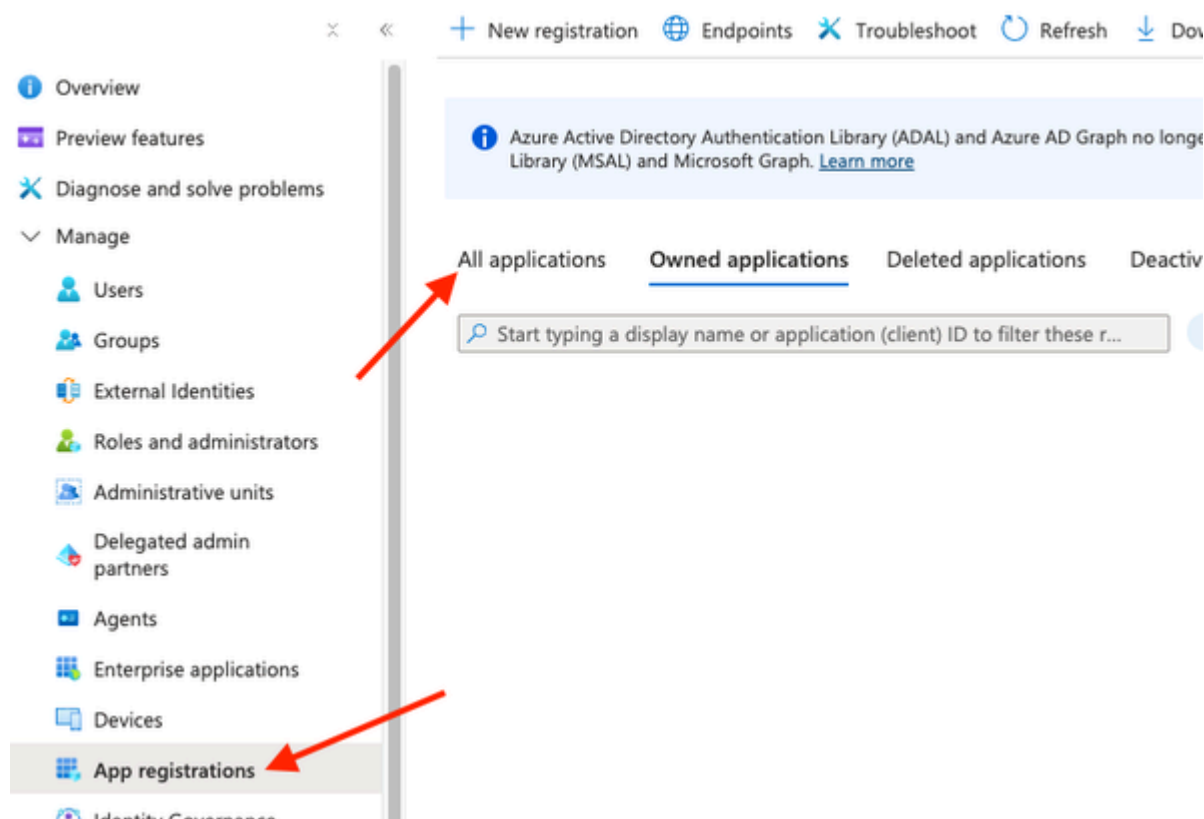


Assegna Utenti E Gruppi All'Applicazione

6) La configurazione di questa applicazione enterprise continua nei passi successivi.

Passaggio 2: Configura registrazioni app Entra ID

1) Tornare a Entra ID e dal menu di navigazione a sinistra, scegliere Registrazioni app. Fare clic sul filtro Tutte le applicazioni e cercare il nome assegnato all'applicazione enterprise. Fare clic sull'applicazione appropriata.



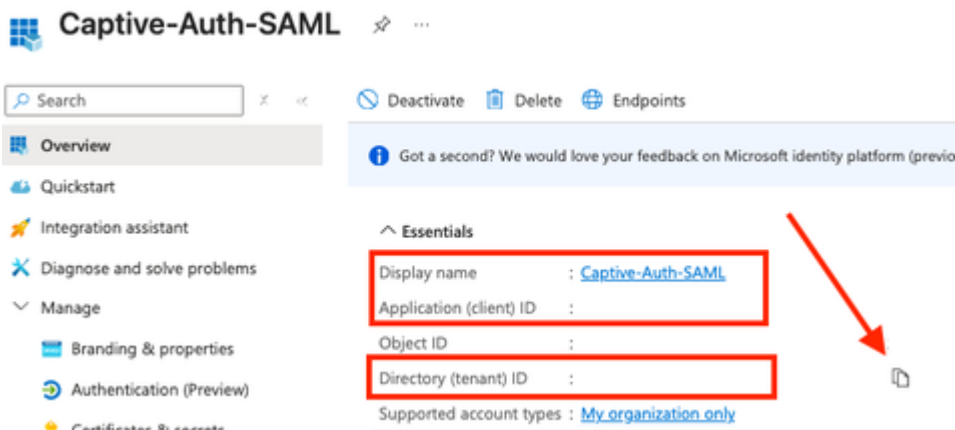
Passa Alle Registrazioni Dell'App E A Tutte Le Applicazioni

2) Raccogliere e annotare i valori Essentials nella registrazione dell'app aziendale.



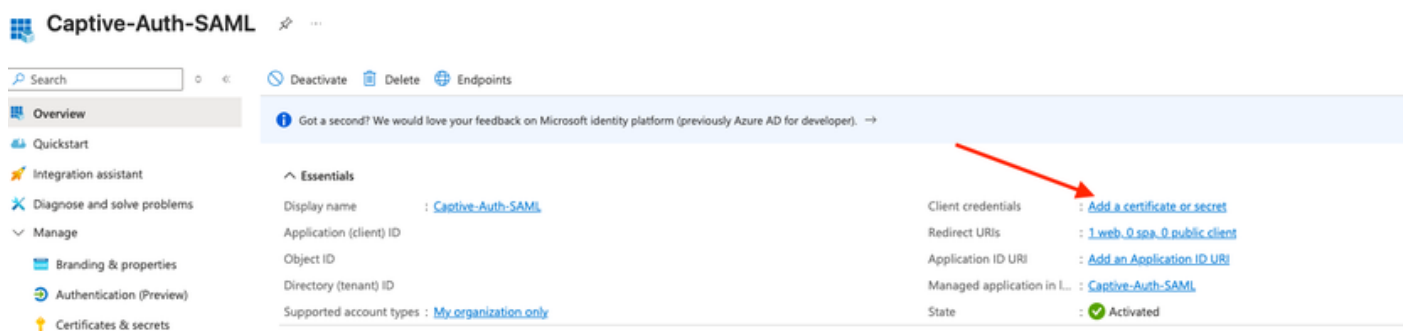
Importante: Passare il mouse sui valori per visualizzare Copia negli Appunti e raccogliere i valori in Essentials nella pagina Panoramica:

- Nome visualizzato
- ID applicazione (client)
- ID directory (tenant)



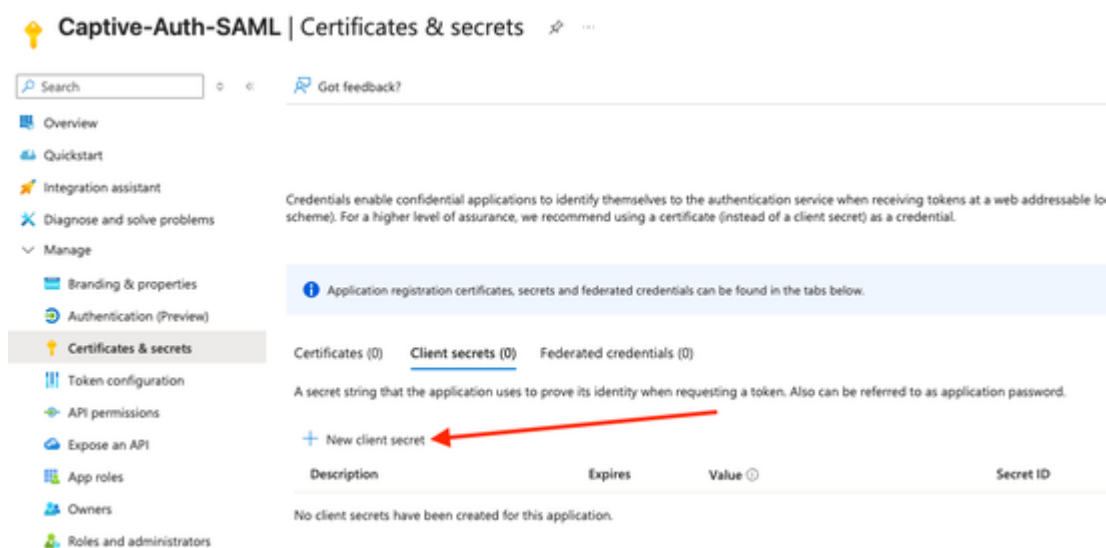
Raccogli Valori Di ID Di Applicazioni E Directory Di Visualizzazione E

3) Fare clic sul collegamento ipertestuale Aggiungi certificato o segreto.



Aggiungi certificato o collegamento ipertestuale segreto

4) Fare clic su + Nuovo segreto client.



Aggiungi nuovo segreto client

5) Fornire una descrizione per il segreto e modificare la scadenza se necessario. Fare clic su Add.

Add a client secret ✕

Description

Expires Recommended: 180 days (6 months) ▾

Add Cancel

Fornire Una Descrizione Per Il Segreto Client

Captive-Auth-SAML | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

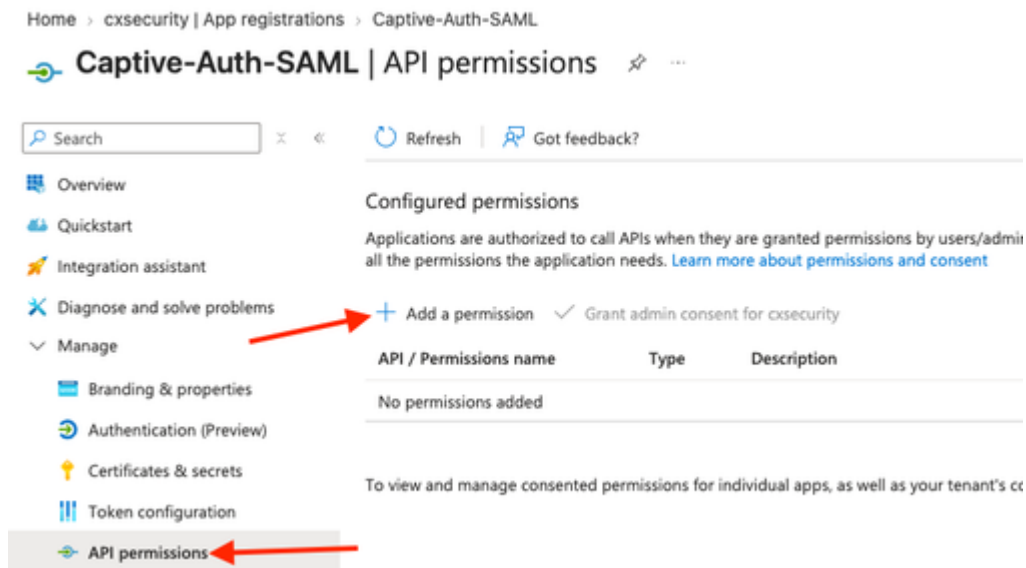
+ New client secret

Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

Copia valore segreto client

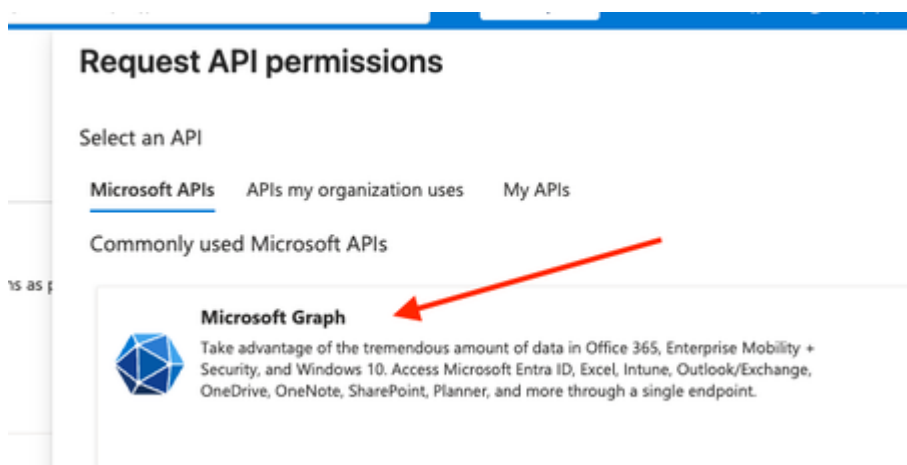
Passaggio 3. Configurare le autorizzazioni API di Microsoft Graph per la registrazione dell'app.

1) Scegliere API Permissions dal menu di navigazione a sinistra, quindi fare clic su + Add a permission.



Configura autorizzazioni API

2) Fare clic su Microsoft Graph API.



Seleziona API di Microsoft Graph

3) Concedere le autorizzazioni Utente delegato. Lettura, quindi fare clic su Aggiungi autorizzazioni.

Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions



User.Read

Permission

Admin consent required

> AgentIdUser

> IdentityRiskyUser

▼ User (1)



User.Read ⓘ

Sign in and read user profile

No



User.Read.All ⓘ

Read all users' full profiles

Yes



User.ReadBasic.All ⓘ

Read all users' basic profiles

No

Add permissions

Discard

Concedi autorizzazioni di lettura agli utenti delegati

4) Concedi utente applicazione.Leggi.Tutte le autorizzazioni (selezionare la casella di controllo).

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

User.Read.All

Permission

Admin consent required

> IdentityRiskyUser

▼ User (1)

☒	User.Read.All ⓘ Read all users' full profiles	Yes
-------------------------------------	--	-----

Concedi all'applicazione tutte le autorizzazioni

5) Cercare e selezionare la casella di controllo Group.Read.All per concedere anche le autorizzazioni di lettura di gruppo. Fare clic su Aggiungi autorizzazioni.

Select permissions

[expand all](#)

Group.Read.All

Permission

Admin consent required

▼ Group (1)

☒	Group.Read.All ⓘ Read all groups	Yes
-------------------------------------	-------------------------------------	-----

Add permissions

Discard

Salva autorizzazioni API

6) Confermare che le autorizzazioni configurate siano allineate e concedere il consenso amministrativo.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for

Concedi Consenso Amministrativo Per Le Autorizzazioni

7) Viene mostrato l'output, una volta ottenuto il consenso dell'amministratore.

+ Add a permission

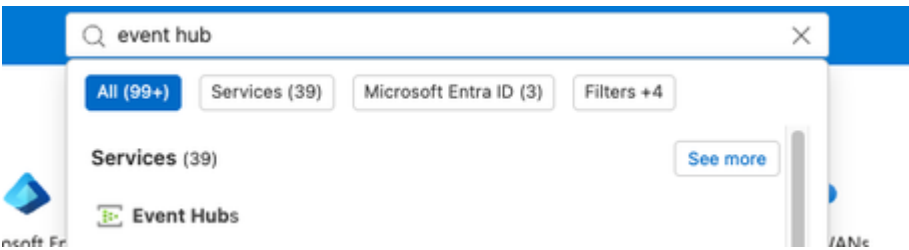
✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✔ Granted for
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for

Output concesso consenso amministrativo

Passaggio 4: Configurare lo spazio dei nomi EH (Event Hub)

1) Cercare e fare clic su Hub eventi.



Configurazione hub eventi di ricerca

2) Creare un nuovo spazio dei nomi EH.



No event hubs namespaces to display

An Event Hubs namespace is a management container for event hubs which provides DNS-integrated network endpoints and a range of access control and network integration management.



[Learn more about Event Hubs](#)

Crea spazio dei nomi hub eventi

3) Configurare lo spazio dei nomi EH.



Nota: È necessario scegliere il piano tariffario Standard o superiore. Il piano tariffario di base impedisce l'utilizzo del realm.

Vedere la [documentazione di Hub eventi di Azure](#) per un'ulteriore valutazione delle impostazioni avanzate di Hub eventi e dell'applicabilità alle esigenze specifiche.

Fare clic su Rivedi + Crea.



Create Namespace

Event Hubs

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + create](#)

Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

[Create new](#)

Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name * ☐ .servicebus.windows.net

Region * ☐ The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more](#)

Pricing tier * ☐ [Browse the available plans and their features](#)

Throughput Units *

Enable Auto-Inflate ☐

[Review + create](#)

< Previous

Next: Advanced >

Configura impostazioni spazio dei nomi hub eventi

4) Una volta completata la convalida, fare clic su Crea.

Home > Event Hubs

Create Namespace

Event Hubs

Validation succeeded.

Basics Advanced Networking Tags Review + create

Event Hubs Namespace
by Microsoft

Basics

Namespace name	captive-auth-ad-eh
Subscription	
Resource group	
Region	East US
Pricing tier	Standard
Throughput Units	1
Availability Zones (Zone Redundancy)	Enabled
Auto-Inflate Maximum Throughput Units	Disabled

Networking

Connectivity method	Public access
Network Protocol Preference	IPv4 only

Security

Minimum TLS version	1.2
Local Authentication	Enabled

[Create](#) [< Previous](#) [Next >](#)

Crea distribuzione spazio dei nomi hub eventi

5) Confermare il completamento della distribuzione, quindi fare clic su Vai alla risorsa.

Home

captive-auth-ad-eh | Overview

Deployment

Search [Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Overview

- Inputs
- Outputs
- Template

Your deployment is complete

Deployment name : captive-auth-ad-eh
Subscription :
Resource group :

> Deployment details

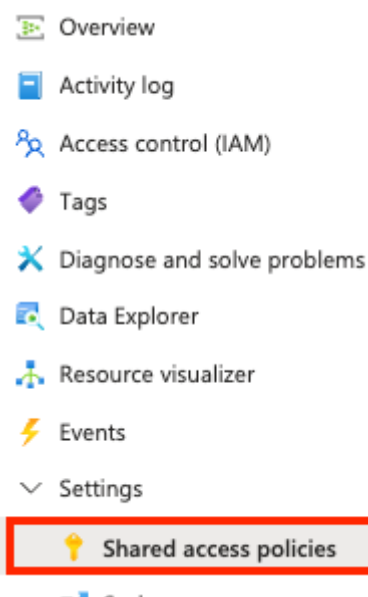
Next steps

[Go to resource](#)

Vai a risorsa spazio dei nomi hub eventi

Passaggio 5: Scegliere o creare criteri di accesso condiviso nello spazio dei nomi dell'hub eventi

1) Dal menu di navigazione a sinistra, scegliere Impostazioni > Criteri di accesso condiviso.

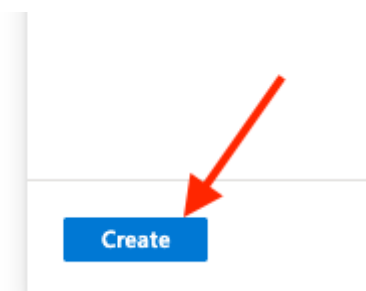


Passa A Criteri Di Accesso Condiviso

2) Fare clic su + Aggiungi e immettere il nuovo nome del criterio, quindi selezionare la casella di controllo Gestisci. Fare clic su Crea nella parte inferiore del pannello dei menu Aggiungi criterio di firma di accesso condiviso.



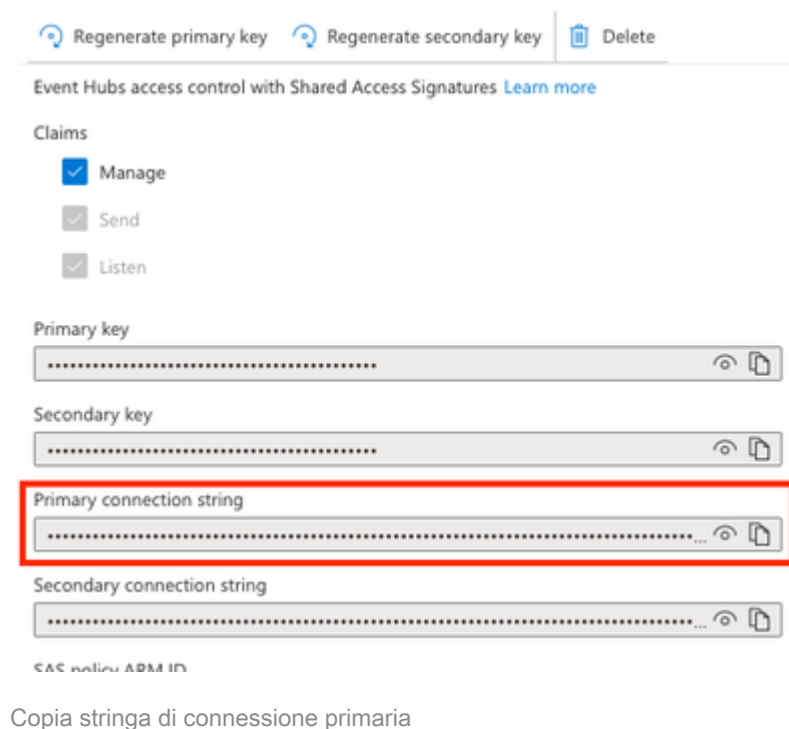
Aggiungi nuovo criterio di accesso condiviso



Crea criteri di accesso condiviso

Passaggio 6: Raccogliere e annotare informazioni sulla firma di accesso condiviso (SAS) dallo spazio dei nomi EH

1) Fare clic sul nuovo criterio di accesso condiviso; la policy EH SAS viene visualizzata nel pannello laterale a destra.



Regenerate primary key Regenerate secondary key Delete

Event Hubs access control with Shared Access Signatures [Learn more](#)

Claims

- ☒ Manage
- ☐ Send
- ☐ Listen

Primary key

Secondary key

Primary connection string

Secondary connection string

CAS policy ABM ID

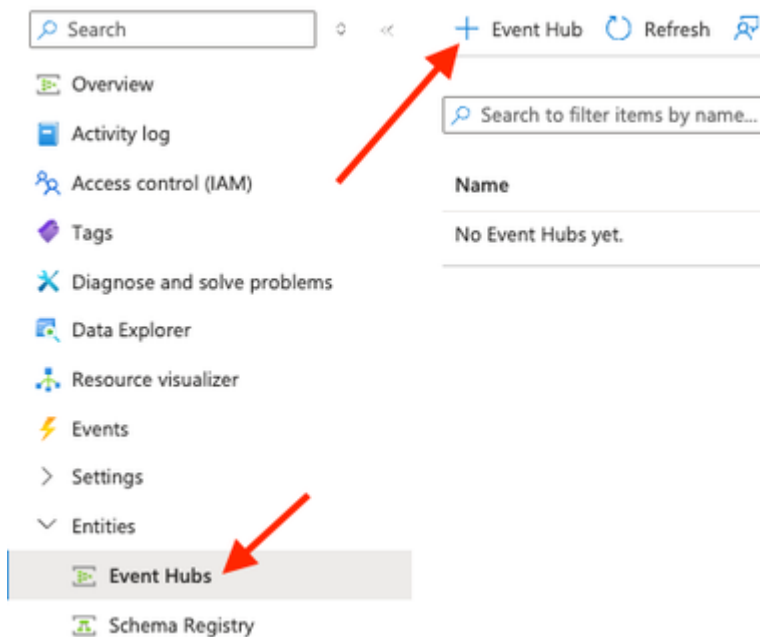
Copia stringa di connessione primaria



Importante: Copiare e annotare la stringa di connessione Primary.

Passaggio 7: Creare un'istanza dell'hub eventi nello spazio dei nomi dell'hub eventi

1) Dal menu Spazio dei nomi, scegliere Entità > Hub eventi. Fare clic su + Hub eventi per creare una nuova istanza EH.



Crea nuova istanza hub eventi

2) Assegnare un nome alla nuova istanza EH, quindi fare clic su Rivedi + crea.

Home > Event Hubs > captive-auth-ad-eh | Event Hubs

Create Event Hub

Event Hubs

Basics Capture Review + create

Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name * ⓘ captive-auth-ad-eh-1 ✓

Partition count ⓘ 1

Retention

Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy ⓘ Delete

Retention time (hrs) * ⓘ 1
min. 1 hour, max. 168 hours (7days)

[Review + create](#) < Previous Next: Capture >

Assegna nome all'istanza dell'hub eventi

3) Una volta completata la convalida, fare clic su Crea per effettuare il provisioning dell'istanza dell'hub eventi.

Create Event Hub ...

Event Hubs

✓ Validation succeeded.

Basics Capture Review + create

Event Hubs Instance
by Microsoft

Basics

Name	captive-auth-ad-eh-1
Partition count	1

Retention

Cleanup policy	Delete
Retention time (hrs)	1

Capture

Capture Status	Off
----------------	-----

Create < Previous Next >

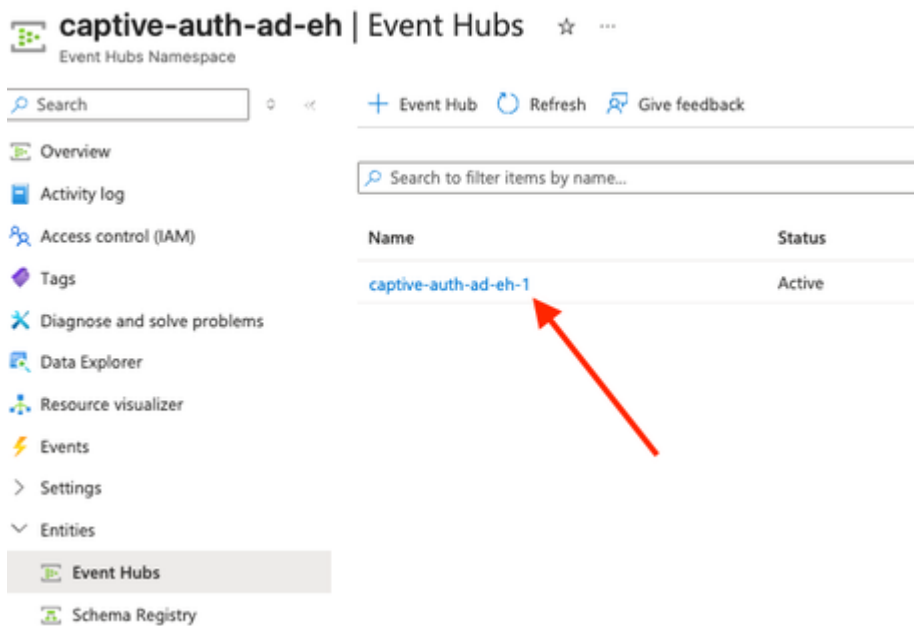
Istanza hub eventi di provisioning



Importante: Copiare e annotare il nome dell'istanza dell'hub eventi.

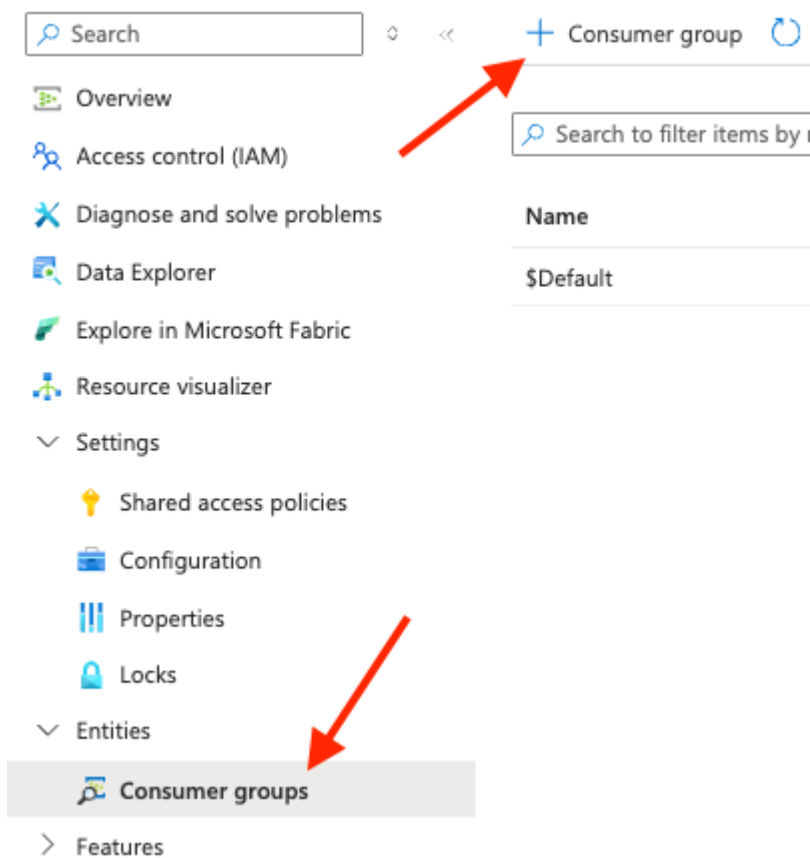
Passaggio 8: Creare un gruppo di consumer dell'istanza dell'hub eventi nello spazio dei nomi dell'hub eventi

1) Fare clic sulla nuova istanza EH configurata nel passaggio precedente.



Configurazione istanza hub eventi di Access

2) Dall'istanza EH, scegliere Entità > Gruppi di consumer, quindi creare un nuovo gruppo di consumer.



Crea gruppo di consumer

3) Assegnare un nome al gruppo di consumer e fare clic su Crea.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Assegna nome al gruppo di consumer



Importante: Copiare e annotare il nome del gruppo di consumer dell'istanza dell'hub eventi.

Passaggio 9: Verifica valori raccolti

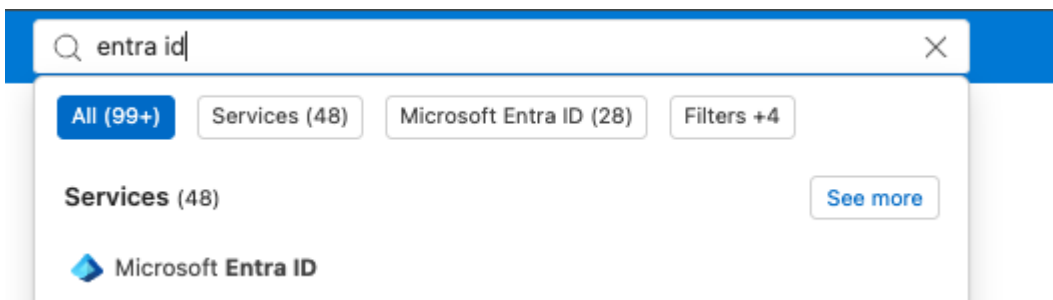
1) A questo punto, si devono prendere in considerazione i valori indicati nei punti precedenti. Se non è stato registrato alcun valore, fare riferimento alla fase in cui è stato raccolto:

- Fase 3, passaggio 2 - Registrazione dell'app (dell'app Enterprise creata per questo processo, a cui fa riferimento il nome visualizzato raccolto)
 - Fase 2, Fase secondaria 2
 - Nome visualizzato
 - ID applicazione (client)
 - ID directory (tenant)
 - Fase 2, Fase secondaria 6
 - Segreto client
- Fase 3, passaggio 6 - Hub eventi
 - Fase 6, Fase secondaria 1
 - Spazio dei nomi EH

- Stringa di connessione primaria
- Fase 7, Fase secondaria 3
 - Nome istanza EH (hub eventi)
- Passaggio 8, Passaggio Secondario 3
 - Nome gruppo di consumer EH

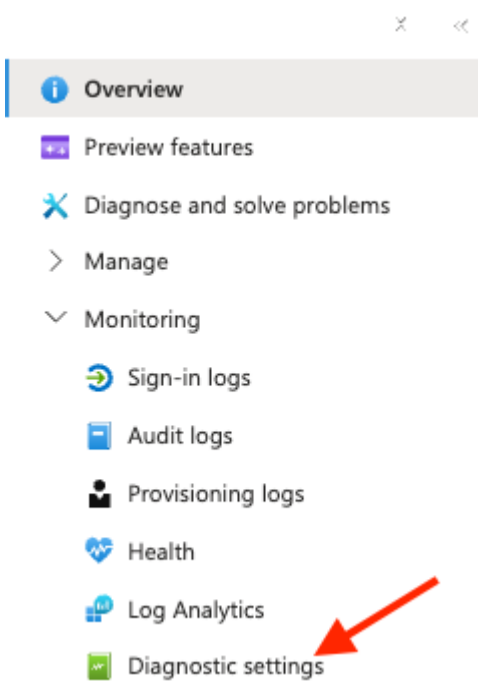
Passaggio 10: Configura streaming registro di controllo ID entri nell'hub eventi

1) Tornare alla configurazione Entra ID tenant.



Cerca E Passa Alla Configurazione Del Tenant Dell'ID Entra

2) Dal menu a sinistra, scegliere Monitoraggio > Impostazioni diagnostiche.



Monitoraggio delle impostazioni di diagnostica

3) Scegliere Impostazioni diagnostica > Generale e fare clic su + Aggiungi impostazione diagnostica.

Diagnostic settings | General



Can you explain how to send diagnostic logs?

Refresh Feedback

Diagnostic settings

General

Custom security attributes

Diagnostic settings are used to configure streaming export of platform logs

Diagnostic settings

Name	Storage account
	-
	-
	-

+ Add diagnostic setting

Aggiungi nuova impostazione diagnostica

4) Assegnare il nome richiesto all'impostazione di diagnostica, selezionare la casella di controllo AuditLogs per eseguire il log e selezionare la casella di controllo Stream to an event hub. Fare riferimento ai valori annotati nelle configurazioni precedenti e al termine fare clic su Salva.

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

captive-portal-auth

Logs

Categories

- ☒ AuditLogs
- ☐ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs

Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

Event hub namespace *

captive-auth-ad-eh

Event hub name (optional) ⓘ

captive-auth-ad-eh-1

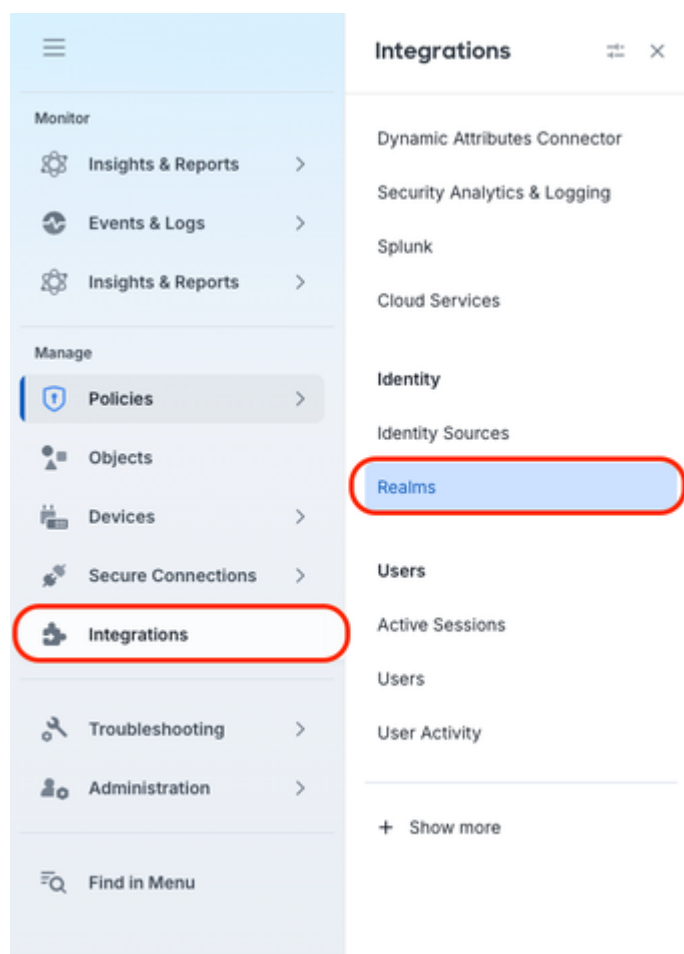
Event hub policy name

☐ Send to partner solution

Fase 4: Consolidamento della configurazione di Azure e dell'autenticazione attiva FMC/FTD

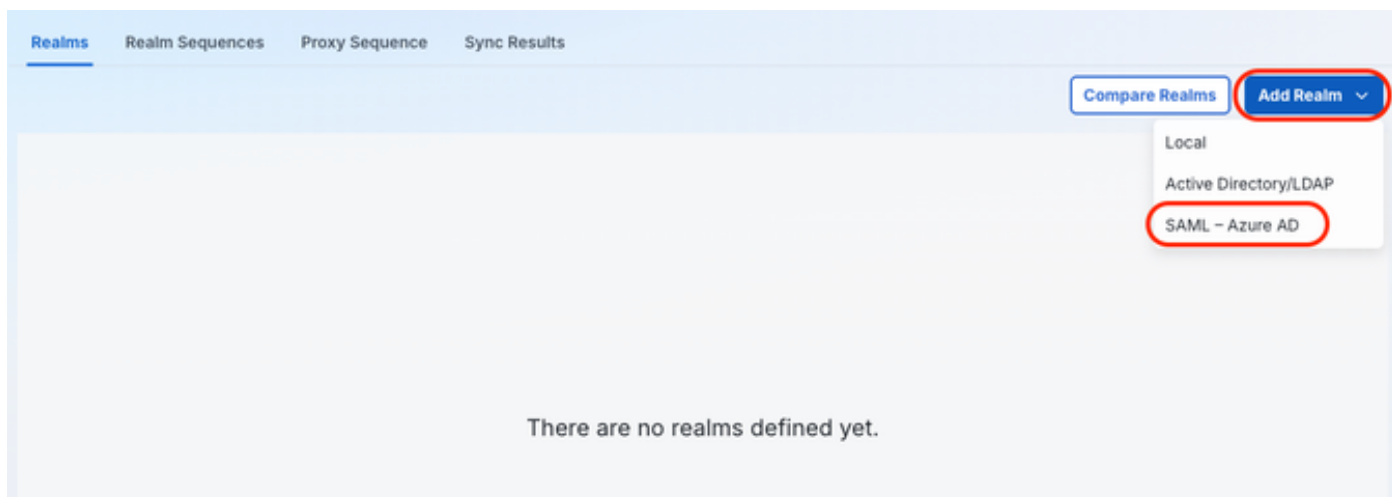
Passaggio 1: Configurare il realm di Azure SAML/Entra ID utilizzando la procedura guidata FMC

1) In FMC, scegliere Integrazioni > Identità > Realm.



Configurazione realm di identità

2) Fare clic su Aggiungi realm nell'elenco a discesa e scegliere SAML - Azure AD.



Aggiungi area di autenticazione di Azure AD SAML

3) Assegnare un nome e una descrizione all'area di autenticazione di Azure per descriverne l'utilizzo e assicurarsi che l'autenticazione passiva con Azure AD o l'utilizzo del portale captivo con Azure AD sia selezionata dall'elenco a discesa Tipo di configurazione. Fare clic su Next (Avanti).

Configurare le impostazioni del realm di Azure AD

4) Scegliere l'oggetto FQDN configurato in precedenza come URL di base. Immettere l'ID entità nel formato di stringa indicato:

https://<fqdn-base-url>/<uniqueSuffix>

- Quando viene configurato il suffisso ID entità SAML (sottolineato in verde nell'esempio di configurazione seguente), assicurarsi che il suffisso sia univoco tra le altre implementazioni SSO all'interno dell'ambiente. Questo valore deve corrispondere anche alla configurazione SAML di Azure. L'URL di base rimane lo stesso per tutta la configurazione.
- L'URL di Assertion Consumer Services (ACS) viene popolato automaticamente e non è modificabile.
- Scegliere il certificato del provider di servizi (SP) registrato nei passaggi precedenti del flusso di lavoro in FMC in Dispositivi > Certificati.
- Dopo aver immesso questi valori, fare clic su Scarica metadati provider di servizi per semplificare il processo di configurazione e confermare che i valori previsti sono stati scritti in Azure.

Add SAML – Azure AD Realm

1 Realm Details Edit

Name	azure-entra-saml
Description	Active Authentication IdP
Identity Provider	Azure AD
Configuration Type	Authenticate passively with Azure AD or using captive portal with Azure AD

2 SAML Service Provider (SP) Metadata

Base URL *

active_auth_fqdn ⓧ ⌵ +

Must resolve to the interface(s) of source security zones used in an identity policy.

Entity ID *

https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID 📋

Unique, alphanumeric identifier for a SAML entity.

Assertion Consumer Services (ACS) URL *

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tgname=azure-entra 📋

URL at which the service provider receives SAML assertions from Azure AD.

Service Provider Certificate *

FTD-SP-Cert ⓧ ⌵ +

Certificate used for SAML authentication and TLS/SSL communication with the secure threat defense device. The certificate must have the value you specify for Base URL that must match the Common Name (CN) or Subject Alternative Name (SAN). The certificate, which must be in PKCS12 format, must be trusted by clients.

[Download Service Provider Metadata](#)

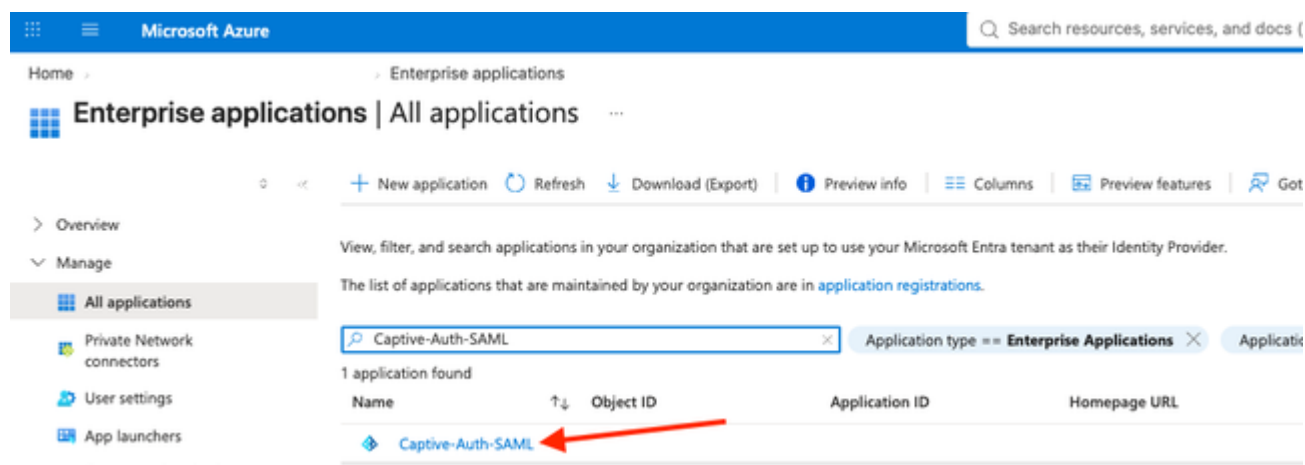
Next

Configurazione dell'URL di base e dell'ID entità e download dei metadati SAML

5) Fare clic su Next (Avanti) per passare alla sequenza 3 della configurazione del realm.

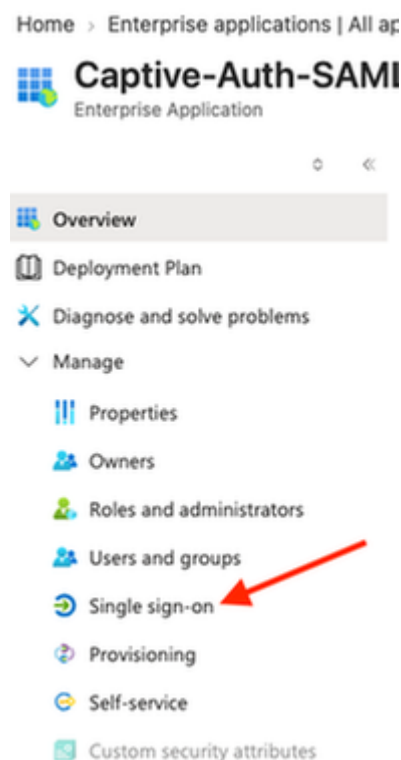
Passaggio 2: Implementare i metadati di SP SAML configurati da FMC nell'applicazione Azure Enterprise

1) Tornare ad Azure e scegliere Entra ID > Gestisci > Applicazioni enterprise. Cercare l'istanza creata in precedenza dell'applicazione Microsoft Entra SAML Toolkit Enterprise.



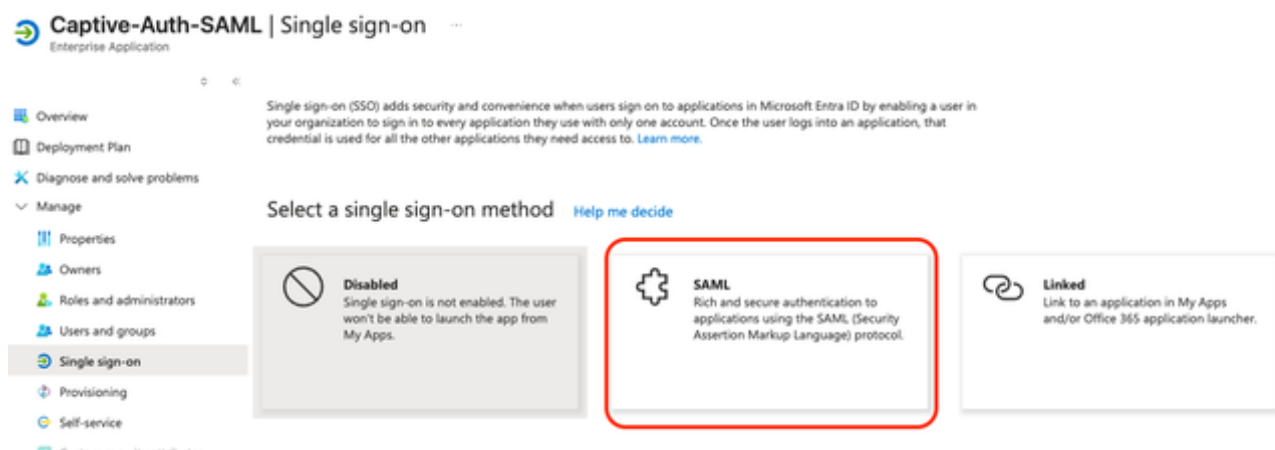
Individuazione applicazione Microsoft Entra SAML Toolkit

2) Dal menu di navigazione laterale, scegliere Gestisci > Single Sign-On.



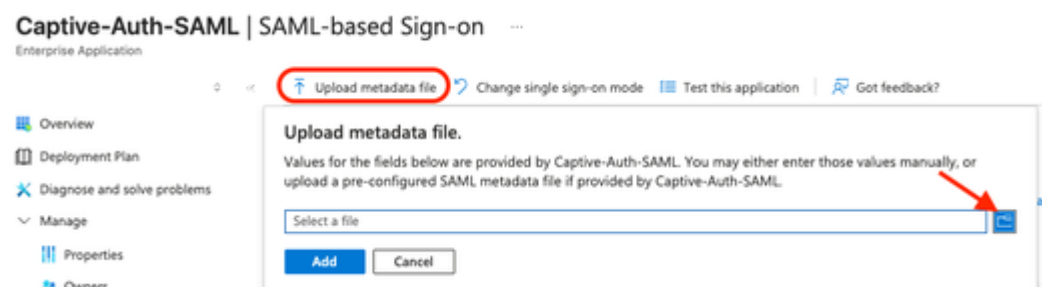
Gestisci configurazione Single Sign-On

3) Fare clic sulla modalità SAML Single Sign-On (SSO).



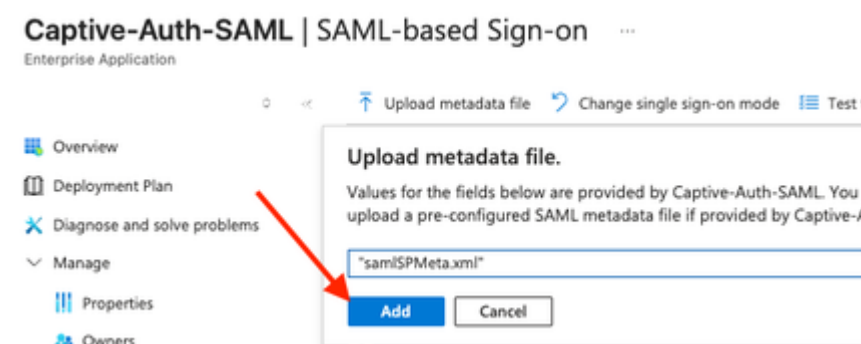
Selezione modalità Single Sign-On SAML

4) Fare clic su Upload metadata file (Carica file metadati) e fare clic sull'icona blu della cartella per cercare nel file system locale il file di metadati SAML scaricato dal FMC.



Caricamento Di File Di Metadati Da Centro Gestione Firewall

5) Una volta completato il caricamento, fare clic su Add (Aggiungi).



Aggiungi applicazione di configurazione SAML

6) Viene visualizzato il pannello laterale per la configurazione SAML di base e valori quali l'identificatore (ID entità) e l'URL ACS vengono estratti dal file XML dei metadati SP originato da FMC caricato e applicato automaticamente. Tuttavia, l'URL di accesso non viene popolato ed è

obbligatorio prima del salvataggio.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID	☒ ⓘ

Add identifier

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tgname=azure-entra-saml	0	☒ ⓘ

Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Patterns: https://samltoolkit.azurewebsites.net/

- ⊗ Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)
- ⊗ This field is required

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

7) Usare il modello di URL per l'accesso fornito, copiare e incollare il valore, quindi fare clic su Salva in alto al termine dell'operazione.

Basic SAML Configuration



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

<https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID> ✓



[Add identifier](#)

Patterns: <https://samltoolkit.azurewebsites.net>

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

<https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tname=azure-entra-saml>

0



[Add reply URL](#)

Patterns: <https://samltoolkit.azurewebsites.net/SAML/Consume>

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

<https://samltoolkit.azurewebsites.net/> ✓

Patterns: <https://samltoolkit.azurewebsites.net/>

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

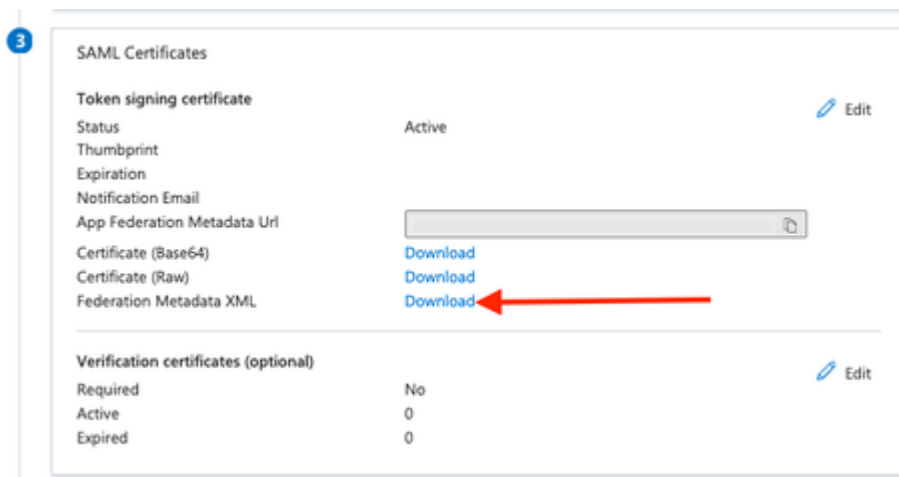
Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url



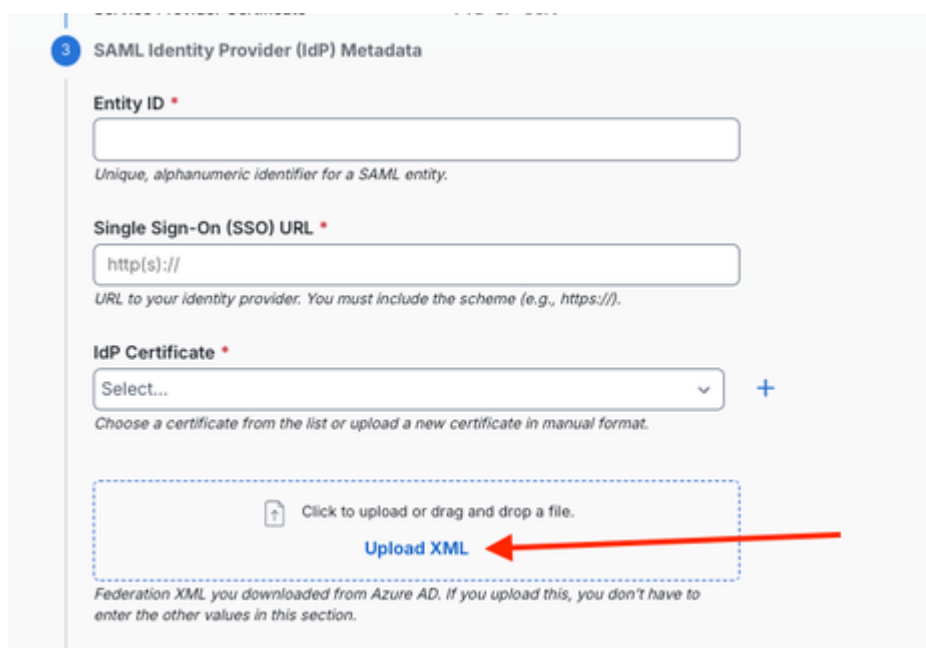
Scorrere verso il basso fino a Certificati SAML ed esportare il file XML dei metadati federativi generati da Azure per l'importazione in Cisco Secure FMC.



Esporta file XML metadati federazione

Passaggio 3: Configurare il realm di Azure SAML/Entra ID utilizzando la procedura guidata di Gestione risorse cluster (continua)

1) Tornare al CCP. Nella sequenza 3, Metadati IdP (SAML Identity Provider), caricare il file XML dei metadati federativi esportati scaricato da Azure in FMC per popolare automaticamente i valori necessari.



Carica file XML metadati federazione

2) Una volta caricati, i valori vengono popolati come mostrato.

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *
  
Choose a certificate from the list or upload a new certificate in manual format.

 Click to upload or drag and drop a file.
Upload XML

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.



Valori provider di identità SAML popolati automaticamente



Nota: Nell'immagine viene visualizzata un'uscita parziale.

3) Inserire i valori raccolti durante l'intero processo di implementazione fino a questo punto:

- Registrazione app
 - ID applicazione (client)
 - Segreto client
 - ID directory (tenant)
- Hub eventi
 - Nome host spazio dei nomi EH
 - Stringa di connessione primaria dello spazio dei nomi EH
 - Nome istanza EH (hub eventi)
 - Nome gruppo di consumer EH

Add SAML – Azure AD Realm



4 Azure AD Details

Client ID *
851607f9-969f-4fed-90ec-829607c1c
Application ID (also referred to as client ID you created in Azure AD).

Client Secret *
.....
Secret string that the application uses to prove its identity when requesting a token.

Tenant ID *
af42bac0-52aa-429f-92db-9258199f
Microsoft Entry ID entity that typically encompasses an organization. Displayed in Azure Entra ID → Properties.

Event Hubs Host Name *
captive-auth-ad-eh.servicebus.windows.net
Hostname of the Event Hub Namespace. Displayed in Event Hubs → Event Hubs Namespace.

Event Hub Name *
captive-auth-ad-eh
Name of your event hub. Displayed in Event Hubs Name Space → Overview.

Consumer Group Name *
captive-auth-ad-eh-cg
A view of an entire event hub. Consumer groups enable consuming applications to each have a separate view of the event stream.

Event Hub Connection String *
Endpoint=sb://captive-auth-ad-eh.servicebus.windows.net/;SharedAccessKeyName=...
Event Hub Connection String: Unique identifier for the event hub (also referred to as topic or endpoint). It is displayed on the Azure AD portal in Event Hubs → (name of your event hub) → Shared access policies → (name of policy).

USER GROUPS ☒
☐ Excluded User Groups
☒ Included User Groups
Enter each group name on a separate line
active-auth-lab
Enter one or more groups from which to download users for identity control. Users in these groups will be available for use in access control policies.

Test

Test connection succeeded

Next

Immettere Le Informazioni Dell'Hub Eventi E Dell'Applicazione

Dopo l'immissione, fare clic su Test per verificare la connessione e verificare che Azure sia raggiungibile con le informazioni fornite.



Nota: Se applicabile, verificare che i gruppi di utenti esclusi/inclusi siano allineati alla configurazione Entra

4) Il passaggio finale della procedura guidata consente di configurare il timeout di SAML Captive Portal Users. L'impostazione predefinita è 1440 minuti.

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

Configura timeout Captive Portal

5) Fare clic su Next (Avanti) per continuare.

After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the management center as Unknown (except for Failed Captive Portal Users).

Next

Sposta avanti con la configurazione del realm di Azure AD

6) La procedura guidata fornisce un riepilogo della configurazione implementata. Fare clic su Salva alla fine del riepilogo dopo che i valori immessi sono stati convalidati e confermati.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

Pulsante Salva riepilogo configurazione realm

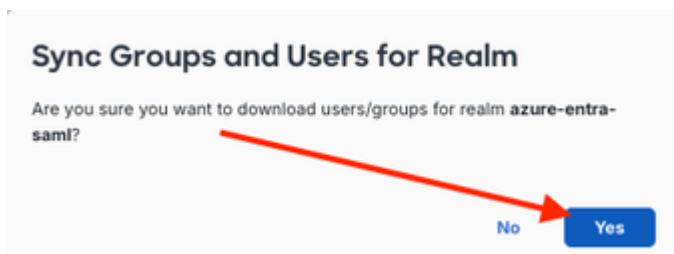
Passaggio 4: Controlla utenti scaricati

1) Confermare che gli utenti possano essere scaricati da Azure Entra con il pulsante Scarica ora nel flusso di lavoro Integrations > Identity > Realms.

Name	Type	Description	Proxy	Status	Value	
azure-entra-saml	SAML - Azure AD (captive portal)	Active Authentication IdP	Not Applicable	Ok	Tenant ID: af42bac0-5	Enabled Download Now

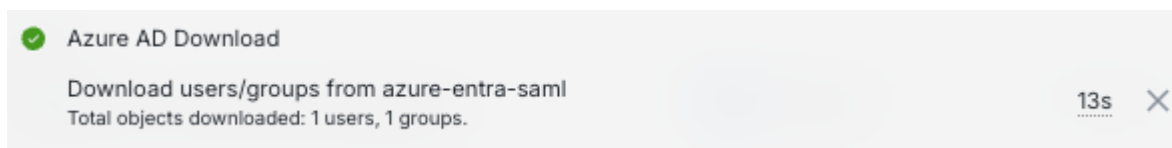
Scarica utenti da Azure AD

2) Fare clic su Yes (Sì) in risposta al prompt della finestra di dialogo.



Conferma download utenti da Azure AD

3) L'operazione di download produce 1 utente e 1 gruppo scaricati, come confermato in Notifiche > Operazioni.

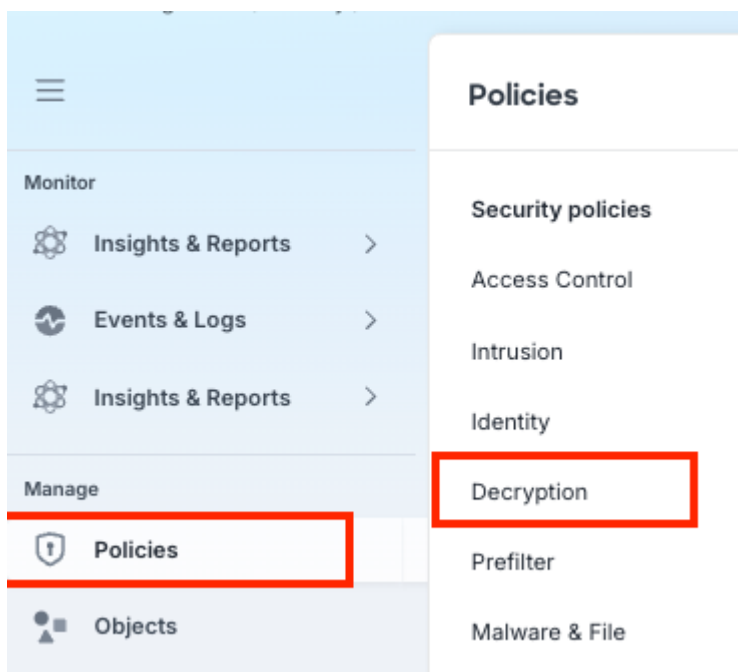


Voce di notifica per il download di utenti da Azure AD

Fase 5: Configurare i criteri in FMC

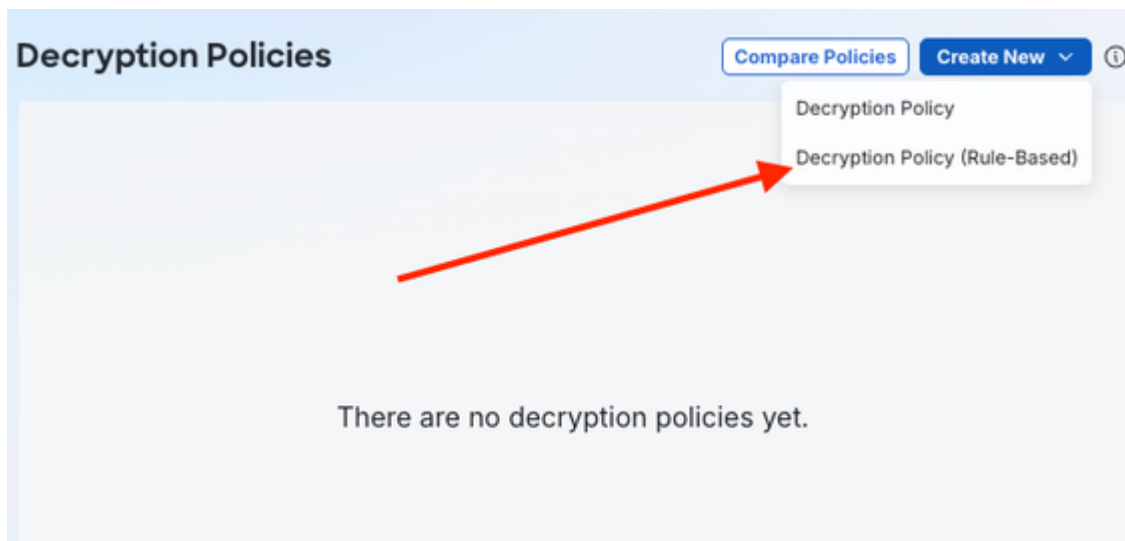
Passaggio 1: Configura criterio di decrittografia

1) In FMC, scegliere Policies > Security Policies > Decryption (Policy di sicurezza > Decrittografia).



Passa Al Criterio Di Decrittografia

2) Fare clic sull'elenco a discesa Crea nuovo e scegliere Criterio di decrittografia (basato su regole).



Crea nuovo criterio di decrittografia basato su regole

3) Assegnare un nome e, se si desidera, una descrizione al nuovo criterio di decrittografia basato su regole e fare clic sull'opzione della scheda Connessioni in uscita (protezione utente) per implementare la funzionalità Decrittografia-abbandono necessaria per l'autenticazione del portale vincolato (autenticazione attiva).

Implementa dettagli criteri connessioni in uscita

4) Scegliere la CA interna applicata in precedenza dall'elenco a discesa applicabile nella stessa finestra di dialogo. Fare clic su Next (Avanti).

5) Personalizzare le opzioni in base alle esigenze.

Create Decryption Policy

1 **Policy Details** Enter name, description, choose policy type and certificates.

2 **Blocking** (Optional) Configure blocking based on TLS version and certificate status

3 **Decryption Exclusions** (Optional) Configure exclusions for outbound connections.

☐ **Block inbound and outbound connections based on TLS version**

We recommend blocking the following because they are not secure. [Reset to default](#)

SSL v3.0 X TLS v1.0 X TLS v1.1 X

☐ **Block inbound and outbound connections based on server certificate status**

We recommend blocking the following because they are not secure. [Reset to default](#)

Invalid Signature X Expired X Not Yet Valid X

Cancel Skip Back **Next**

Personalizza opzioni criteri di decrittografia

6) Nell'esempio, vengono utilizzati i valori predefiniti, ad eccezione dei dettagli di policy obbligatori. Completare la configurazione guidata facendo clic su Crea criterio.

Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Blocking
(Optional) Configure blocking based on TLS version and certificate status

3 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

Decryption Exclusions

☐ Bypass decryption for sensitive URL categories
In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required
URL Categories: Finance Online Trading Health and Medicine [+ Add](#)

☒ Bypass decryption for undecryptable distinguished names
Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.
[56 Distinguished names included](#)

☒ Bypass decryption for undecryptable applications
Certain applications are not supported for decryption due to a variety of reasons (certificate pinning, client certificate authentication, and so on). This option bypasses decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.
[59 Applications included](#)

Intelligent Decryption Bypass

☐ Bypass decryption for very low-risk connections
Bypass decryption for very low-risk clients connecting to trusted servers.
Note: Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients

[New](#)

[Cancel](#) [Skip](#) [Back](#) [Create Policy](#)

Crea criterio di decrittografia finale

Passaggio 2: Configura regole dei criteri di decrittografia

1) Di seguito è illustrato il layout predefinito di un criterio di decrittografia basato su regole. Il traffico che non corrisponde alle regole abilitate predefinite, ad esempio la regola 3 (che fa riferimento a un elenco preallocato di nomi di dominio non decrittografabili) e la regola 6 (che fa riferimento ad applicazioni contrassegnate come non decrittografabili), è soggetto all'azione Decrittografa - abbandona in base alla regola 7. Queste impostazioni predefinite, insieme all'azione predefinita, possono essere modificate in base alle esigenze. Per impostazione predefinita, il traffico che non soddisfa nessun'altra regola è configurato come Non decrittografare.

Il traffico del servizio di autenticazione di Azure non deve essere decrittografato per l'ispezione, quindi è stata creata una regola dedicata. Fare clic su + Aggiungi regola per iniziare.

active-auth-decrypt-policy Save Cancel

Decryption Policy for Active Authentication

[Rules](#) [Trusted CA Certificates](#) [Undecryptable Actions](#) [Advanced Settings](#)

[+ Add Category](#) [+ Add Rule](#)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	Auto-Rule-Certificate-Stz (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Vers	Block with reset
3	Auto-Rule-Undecrypt	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
4	Auto-Rule-Low-Risk-Con (Disabled)	any	any	any	any	any	any	any	any	any	Any (Except L	1 Client Threat	Do not decrypt
5	Auto-Rule-URL-Categoric (Disabled)	any	any	any	any	any	any	any	any	any	Finance (Any Health and M	any Online Tradin	Do not decrypt
6	Auto-Rule-Undecryptabl	any	any	any	any	any	any	Tags: undecry	any	any	any	any	Do not decrypt
7	Auto-Rule-Internal-La	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													Do not decrypt

Aggiungi Regola E Visualizzazione Del Layout Di Decrittografia Predefinito Basato Su Regola

2) Assegnare un nome alla nuova voce della regola di decrittografia, scegliere Non decrittografare dall'elenco a discesa Azione e posizionare la regola nella parte superiore, con regole meno specifiche. Per restringere ulteriormente la regola, vengono implementate anche le zone di origine/destinazione.

Add Rule

Name: ☒ Enabled

Action:

Insert:

[Zones](#) [Networks](#) [VLAN Tags](#) [Users](#) [Client Threat](#) [Applications](#) [Ports](#) [Category](#) [Certificate](#) [DN](#) [Cert Status](#) [Cipher Suite](#) [Version](#) [Logging](#)

Available Zones

- Inside_Zone
- Outside_Zone
- DMZ_Zone

Source Zones (1):

Destination Zones (1):

Cancel Add

Configura regola di non decrittografia

3) Prima di aggiungere la regola, fare clic sulla scheda Applicazioni, cercare e fare clic sull'applicazione del servizio di autenticazione di Azure. Fare clic su Aggiungi alla regola, quindi su Aggiungi.

Add Rule

Name: Azure-Auth-Service-DND ☒ Enabled Insert: above rule 3

Action: Do not decrypt

Zones Networks VLAN Tags Users Client Threat **Applications** Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Application Filters Clear All Filters Available Applications (2) Selected Applications and Filters (0)

Search by name: azure a

Risks (Any Selected)

- ☐ Very Low 809
- ☐ Low 715
- ☐ Medium 2239
- ☐ High 1823
- ☐ Very High 609

Business Relevance (Any Selected)

- ☐ Very Low 009

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Add to Rule

any

Cancel Add

Aggiungi regola applicazione del servizio di autenticazione di Azure

4) Fare clic su Save (Salva).

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes Save Cancel

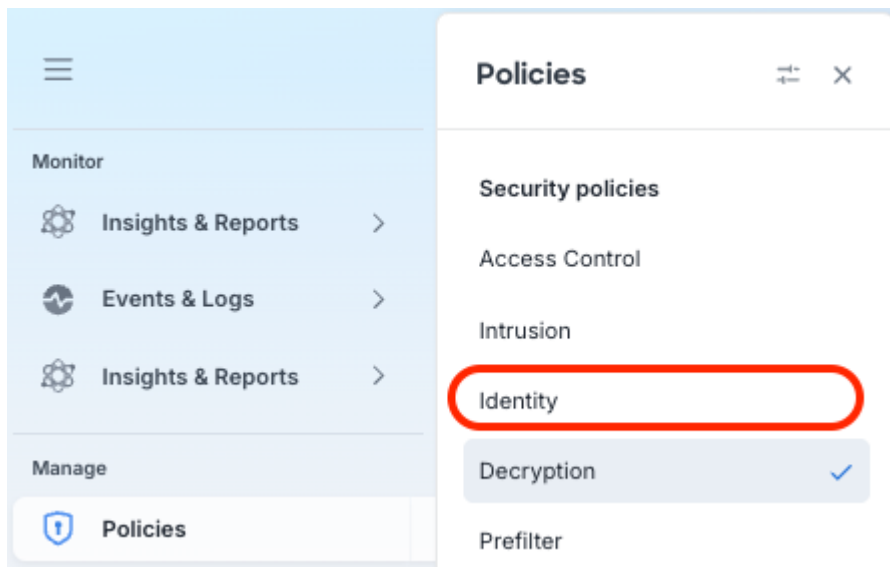
+ Add Category + Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
1	Auto-Rule-Certificate-St (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Ver	Block with reset
3	Azure-Auth-Service-	Inside_Zone	Outside_Zon	any	any	any	any	Azure Authen	any	any	any	any	Do not decrypt

Salva criterio di decrittografia

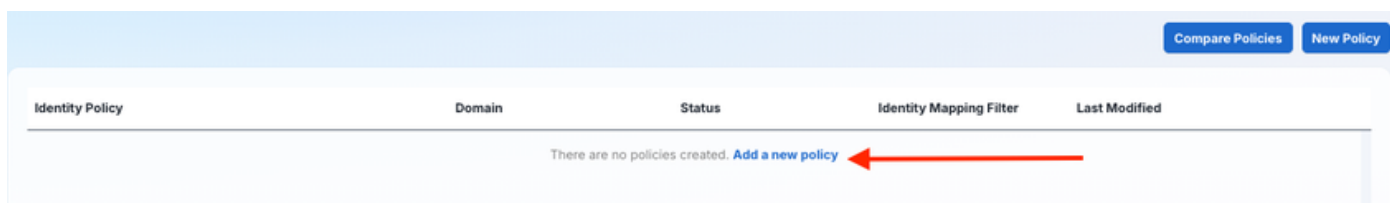
Passaggio 3: Crea criterio di identità

1) Scegliere Criteri > Criteri di sicurezza > Identità per creare un criterio di identità.



Crea criterio di identità

2) Creare un nuovo criterio di identità e fare clic su Aggiungi nuovo criterio.



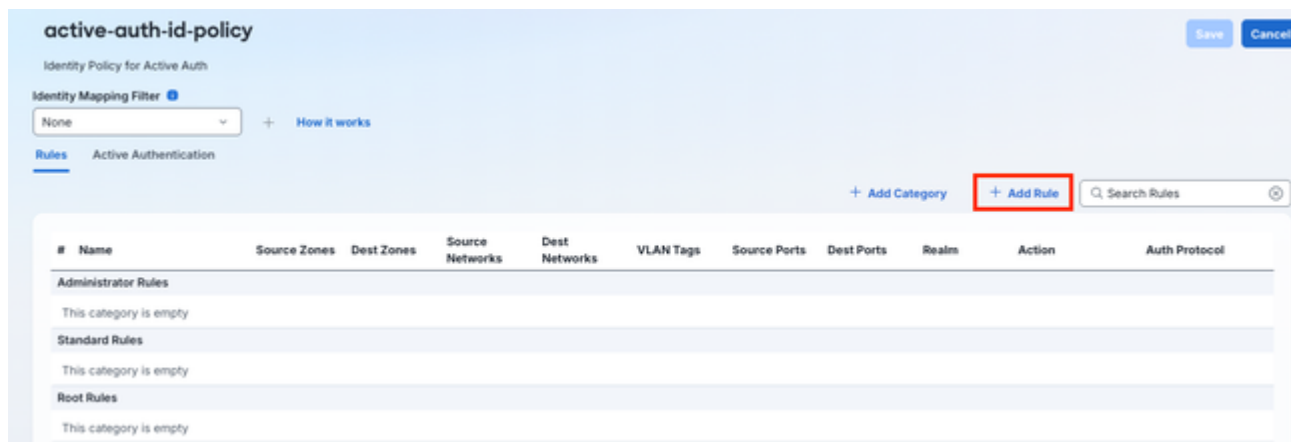
Aggiungi nuova configurazione dei criteri di identità

3) Assegnare un nome e, se applicabile, una descrizione alla nuova politica di identità. Fare clic su Save (Salva).

Nome nuovo criterio di identità

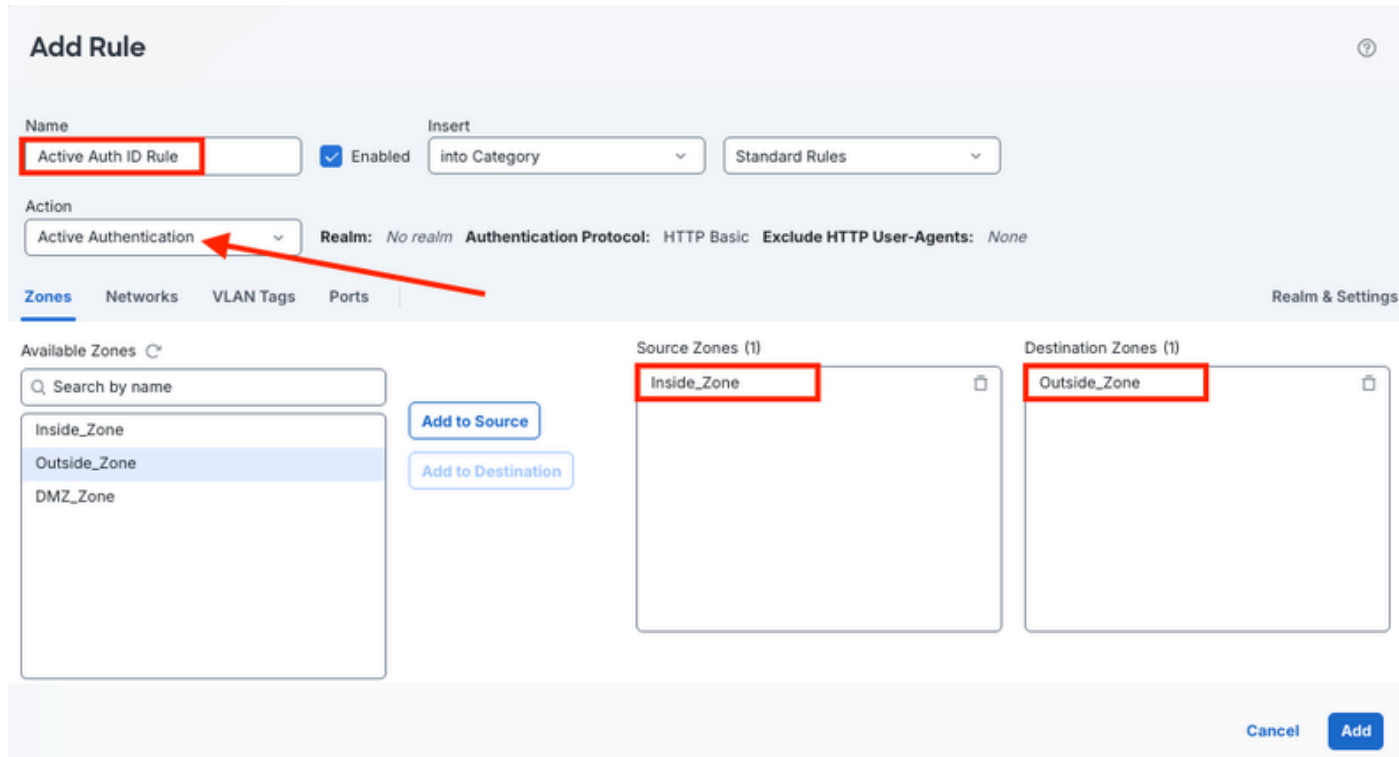
Passaggio 4: Configura regole dei criteri di identità

1) Aggiungere una nuova regola facendo clic su + Aggiungi regola.



Aggiungi nuova regola dei criteri di identità

2) Assegnare un nome alla nuova regola, scegliere Autenticazione attiva dall'elenco a discesa Azione e limitare le zone/reti specifiche che devono corrispondere alla regola per eseguire l'Autenticazione attiva.



Configura impostazioni regole di autenticazione attive

3) Prima di fare clic su Aggiungi, fare clic sulla scheda Realm and Settings (Area di autenticazione e impostazioni) all'interno dell'editor delle regole. Confermare che il realm configurato nei passaggi

precedenti sia stato scelto come realm di autenticazione, quindi fare clic su Aggiungi.

Add Rule

Name: Active Auth ID Rule ☒ Enabled Insert: into Category Standard Rules

Action: Active Authentication **Realm:** azure-entra-saml (S... **Authentication Protocol:** SAML **Exclude HTTP User-Agents:** None

Zones Networks VLAN Tags Ports [Realm & Settings](#)

Authentication Realm *
azure-entra-saml (SAML)

☐ Use passive identity if available.
Active identity realm is going to be used as a passive identity realm.

Authentication Protocol
SAML

▶ HTTP User Agent Exclusions

Cancel Add

Configura Realm E Impostazioni Per La Regola Di Identità

4) La regola viene aggiunta e configurata. Fare clic su Save (Salva).

active-auth-id-policy
Identity Policy for Active Auth

Identity Mapping Filter: None [How it works](#)

Rules Active Authentication

[+ Add Category](#) [+ Add Rule](#) Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (F	any	any	any	any	any	azure-entra-san	Active Authentication	SAML
Root Rules											
This category is empty											

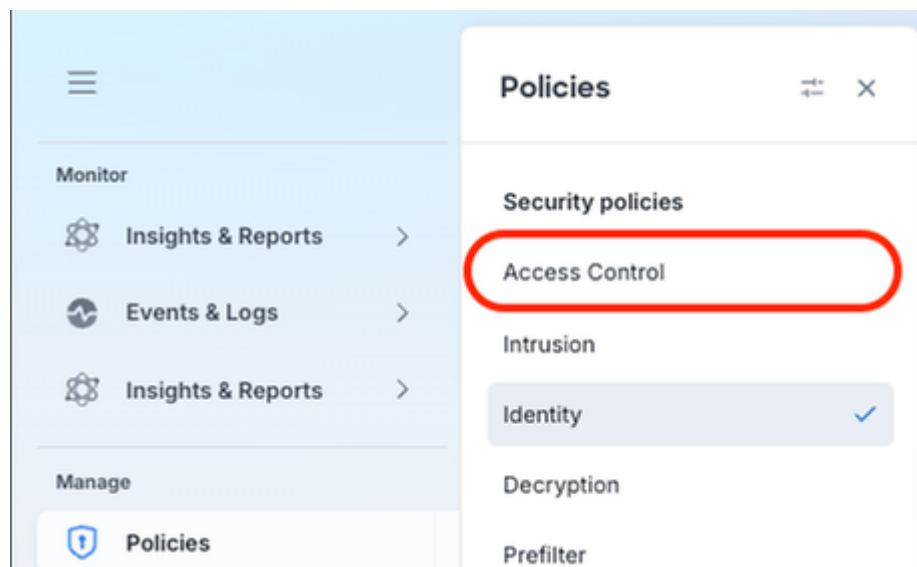
You have unsaved changes Save Cancel

Salva configurazione regole dei criteri di identità

Passaggio 5: Configurare i criteri di controllo di accesso

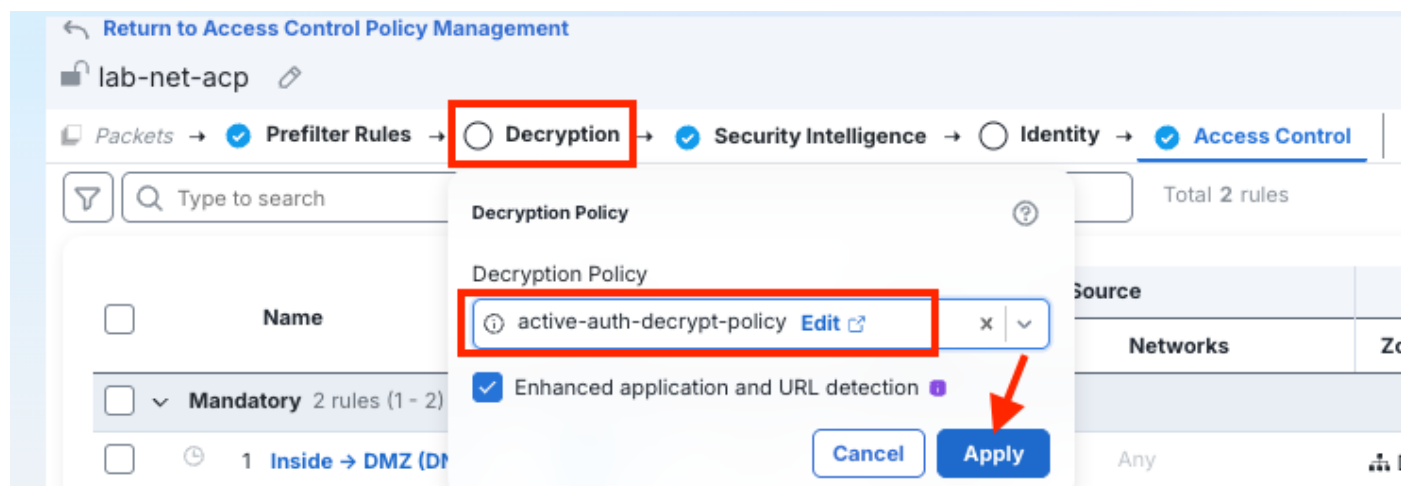
1) Scegliere Criteri > Criteri di sicurezza > Controllo di accesso, quindi fare clic sulla Policy di

controllo di accesso a cui è assegnato l'FTD.



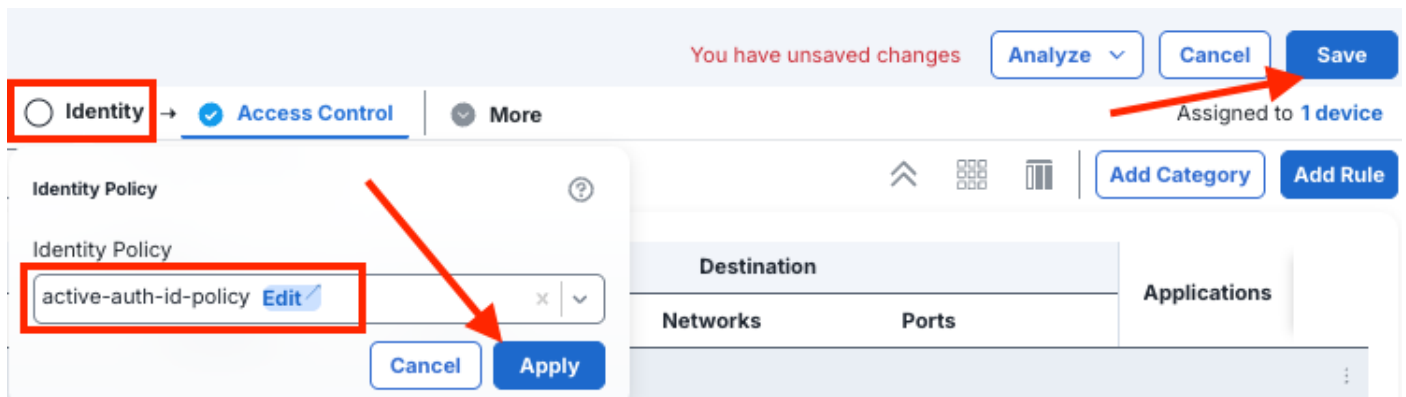
Configurazione dei criteri di controllo dell'accesso

2) Confermare che i criteri di decrittografia configurati nei passaggi precedenti siano applicati ai criteri di controllo dell'accesso.



Applica Criterio Di Decrittografia Al Controllo Di Accesso

3) Confermare che i criteri di identità configurati nei passaggi precedenti siano applicati anche ai criteri di controllo di accesso. Salvare le modifiche ai criteri.



Applica criterio di identità al controllo di accesso

4) Confermare l'esistenza di regole che consentano il traffico dei data plane client attraverso il firewall protetto dopo la riuscita dell'autenticazione attiva. Nell'esempio riportato di seguito viene utilizzato un set di regole più ampio in base all'ambiente lab.

☐	Name	Action	Source		Destination			Applications
			Zones	Networks	Zones	Networks	Ports	
☐ Mandatory 2 rules (1 - 2)								
☐	1 Inside → DMZ (DNS)	Allow	Inside_Zone	Any	DMZ_Zone	Any	Application Default	DNS
☐	2 DMZ-Inside → Outside	Allow	DMZ_Zone Inside_Zone	Any	Outside_Zone	Any	Any	Any
☒ Default (No rules)								

Set di regole di traffico del piano dati utente

Passaggio 6: Distribuire le configurazioni sui dispositivi Cisco Secure Firewall

Dopo la distribuzione, ai client che inviano traffico viene richiesta una pagina Web di accesso Microsoft per eseguire l'autenticazione attiva con Azure Entra.

Per ulteriori informazioni sul processo documentato qui, vedere [Creare un'area di autenticazione SAML \(Microsoft Azure AD\) per l'autenticazione attiva \(portale captive\) - Capitolo: Realm nella Guida alla configurazione dei dispositivi di FMC 10.x](#).

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

GUI

Convalida sessioni utente e attività nel CCP:

- Scegliere Integrazioni > Utenti > Sessioni attive.

The screenshot shows the Cisco Cloud-delivered Firewall Management Center (CCP) interface. The breadcrumb navigation is 'Integrations / Users / Active Sessions'. The left sidebar has 'Monitor' selected. The main content area shows a table of active sessions. A search bar at the top right has a 'Switch to legacy UI' toggle. Below the table, there are buttons for 'Refresh' and 'Delete'.

☐	Login Time	RealmUsername	Last Seen ↓	Authentication Type	Current IP	Session Duration	Realm	Username
☐	2026-10-07 02:10:02	azure-entra-samlcaptive-pc	2026-10-07 02:10:02	Active Authentication		1 min 40 sec	azure-entra-saml	captive-portal-user

Output sessioni attive FMC

- Scegliere Integrazioni > Utenti > Attività utente.

The screenshot shows the Cisco Cloud-delivered Firewall Management Center (CCP) interface. The breadcrumb navigation is 'Integrations / Users / User Activity'. The left sidebar has 'Monitor' selected. The main content area shows a table of user activities. A search bar at the top right has a 'Switch to legacy UI' toggle. Below the table, there are buttons for 'Refresh', 'Delete', and 'Delete All'.

☐	Time ↓	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port
☐	2026-10-07 02:10:02	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		
☐	2026-10-07 02:10:01	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		

Output attività utente FMC

In Azure, passare all'interfaccia di amministrazione di Microsoft Entra:

- Filtra app aziendali, cerca/fai clic sull'app applicabile.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane includes 'Home', 'Favorites', 'Entra ID', 'Overview', 'Users', 'Groups', 'Devices', 'Agents', 'Enterprise apps' (highlighted with a red box), 'App registrations', 'Roles & admins', 'Delegated admin partners', and 'Tenant governance'. The main content area is titled 'Enterprise applications | All applications'. It features a search bar with 'captive-' entered (highlighted with a red box) and a table of applications. The table has columns for 'Name', 'Status', and 'Object ID'. The first application listed is 'Captive-Auth...' (highlighted with a red arrow). Other applications listed include 'Private Network connectors', 'User settings', 'App launchers', and 'Custom authentication extensions'.

Esplorazione app aziendali Entra Admin Center di Azure

- Scegliere Attività > Log di accesso.

Home > Enterprise applications | All applications > Captive-Auth-SAML

 **Captive-Auth-SAML** | Sign-in logs ...

Enterprise Application

«

Download

Export data Settings

Troubleshoot

Refresh

Manage view

Got feedback?

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption
- Activity**
 - Sign-in logs**
 - Usage & insights

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter

Show dates as: UTC

Date range: 10/7/2026 - 10/7/2026

Application contains

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
2026-10-07T06:10:02Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:00Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:59Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:58Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:52Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:51Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:29Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted

Registri attività di accesso applicazione aziendale di Azure

CLI

- Nella CLI FTD è possibile visualizzare le statistiche relative alle risposte SAML e captive portal:

<#root>

>

debug menu captive-portal 6

```
SAML passed requests captive-portal 14
SAML failed requests captive-portal 0
SAML passed responses captive-portal 4
SAML failed responses captive-portal 0
Total captive-portal bee-client messages processed 4
Total captive-portal bee-client messages successful 4
Total captive-portal bee-client messages failed 0
Total bee-client reconnects 0
```

Risoluzione dei problemi

Debug Captive Portal

- Il comando `system support captive-portal-debug` può essere usato sull'FTD. Nell'output viene illustrato come abilitare il debug e vengono annotati i segmenti chiave dell'output per comprendere il flusso del portale vincolato.

```
<#root>
```

```
>
```

```
system support captive-portal-debug
```

```
Enable firewall-debug too? [n]:
```

```
y
```

```
Enable identity-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol:
```

```
tcp
```

```
Please specify a client IP address:
```

```
192.168.20.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Enable daq-debug too? (WARNING: current packet debug configs and logs will be overwritten) [n]:
```

```
Monitoring captive_portal and firewall and identity debug messages
```

```
!---
```

```
Baseline output pending user Captive Portal authentication
```

```
...
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 match rule order 1, id 1 action Captive portal
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 didn't find active binding, initiating captive portal
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 captive portal authentication started
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 defer trust until captive portal redirect is complete
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 Current state = S_INIT, Event = EVT_CP_RULE_MATCH
```

```
...
```

```
!---
```

```
Captive Portal probe intercepted and redirected to SAML IdP (generate_204)
```

```

...
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 AppID session with service_id: 676, url: http
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_PENDING_USER, Event = EVT_
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 app event changes: service, client, host, ur
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 using ipv4 address 192.168.20.1 for redirect
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 encrypted redirect url: https://ftd-inside.e
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_REDIRECTING, Event = EVT_F
...
!---

```

SAML authentication completes, identity binding created

```

...
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 looked for user_id with realm_id 2 auth_type
192.168.20.200 54023 -> 198.51.100.280 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 IdentityFlowSetupEventHandler Retrieved iden
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 New firewall session
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 allow action
...
!---

```

Authenticated binding persists across subsequent, unrelated destinations (no further redirects)

```

...
192.168.20.200 54024 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54025 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54026 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54027 -> 198.51.100.3 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 19935 -> 198.51.100.4 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
...

```

Dump identità utente

- Per creare un'istantanea dei dati sullo stato dell'identità dell'utente corrente sull'FTD, eseguire il comando `system support firewall-engine-dump-user-identity-data` sulla CLI dell'FTD:

```
> system support firewall-engine-dump-user-identity-data
```

Successfully commanded snort.

>

- Nella CLI in modalità expert, durante l'accesso con le credenziali di amministratore locale del dispositivo FTD, visualizzare il contenuto del file scaricato in
/ngfw/var/sf/user_enforcement/user_identity.dump

<#root>

>

expert

admin@ftd:~\$

sudo su

Password:

root@ftd:/home/admin#

root@ftd:/home/admin#

ls -lah /ngfw/var/sf/user_enforcement/user_identity.dump

-rw----- 1 root root 5.6K Oct 7 07:51 /ngfw/var/sf/user_enforcement/user_identity.dump

root@ftd:/home/admin#

root@ftd:/home/admin#

less /ngfw/var/sf/user_enforcement/user_identity.dump

...

IP:USER

!--- Host IP is aligned with the user authenticated via Captive Portal/Active Authentication

Host ::ffff:192.168.20.200

::ffff:192.168.20.200:0 realm 2 type 8, username azure-entra-saml\captive-portal-user@onmicrosoft.examp

::ffff:192.168.20.200: SXP initialized 0 sgt 0

ABP values: None

SXP MAPPING:

...

Problemi possibili

Autorità di certificazione sconosciuta del portale vincolato

Problema: Il browser client restituisce un errore dell'autorità emittente sconosciuta quando viene tentata l'autenticazione.

Probabile causa: L'autorità di certificazione interna non è attendibile nel browser client.

Risoluzione: Verificare che la CA sia attendibile nel browser. L'esempio riportato conferma che il certificato CA interno è attendibile.

Portale vincolato "Server non trovato"

Problema: Quando il browser client tenta di caricare il portale vincolato, restituisce "Server Not Found" (Server non trovato) per l'URL di base durante il tentativo di raggiungere l'URL di base o simili.

Probabile causa: Raggiungibilità DNS o configurazione errata DNS.

Risoluzione: Verificare che il client disponga del server DNS appropriato configurato per risolvere il record A. Verificare che il server disponga di un record A mappato all'FQDN e che sia raggiungibile e reattivo.

Informazioni correlate

- [Creare un'area di autenticazione di Microsoft Azure AD \(SAML\) per l'autenticazione attiva \(portale captive\) - Guida alla configurazione del dispositivo FMC 10.x](#)
- [Documentazione di Hub eventi di Azure](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).